SAFERIDE

OpenSentry
SafeRide open source security project (AGL)
Current AGL Security Status

• AGL security is based on Tizen security:
  • Mandatory Access Control (SMACK)
  • Application Privilege Management and Enforcement via Cynara
  • System hardening recommendations.
  • Others (??)
The Problem

• The previous list contain static solutions that give a solution to security issues we are aware as of today.

• Problem:
  • Difficult to configure and manage.
  • In the security world we need to give a solution to unknown issues as well.
  • How to do that?
Enhancement Proposal

• SafeRide propose to enhance AGL security solution by adding a new feature to the AGL Yocto Layer (can be a standalone layer as well) that will provide Security Control and Monitoring:
  • Control: Remote control of security policy. Add/Remove/Modify security rules.
  • Monitoring: Remote monitoring of system behavior.
Benefits

• OpenSentry will provide a unified and easy to use interface to various the security tools (consolidation). Can be used during development and production phases.
• OpenSentry will allow to monitor security breaches by collecting behavioral logs and uploading them to the cloud.
• OpenSentry will allow to apply virtual patches in case a breach was detected (analysis of collected data).
Deep Dive
Summary

- Questions?