REbus

Philippe Biondi, Xavier Mehrenberger, Sarah Zennou — Airbus Group Innovations

SSTIC — 4–6 juin 2014

AIRBUS
GROUP

REbus

Concept

- Bus de communication
- Échange de messages
- Mettre en relation des agents
- Permettre la simplicité et la modularité des outils

REbus

Exemples d'agents

- Identifieurs de fichiers
- Analyseurs statiques
- Extracteurs de caractéristiques, de CFG
- Sandboxes
- Knowledge bases
- Unpackers
- Honeypots
- Grapheurs
- Interface web
- IDA
- etc.

REbus: format de messages

Descriptor

label	nom commun, nom du fichier d'origine
selector	50% identifiant unique d'un *descriptor*, 50% type MIME
precursors	liste des *selectors* ayant participé à la création de ce *descriptor*
history	liste des agents étant intervenus pour aboutir) ce *descriptor*
value	valeur (ou référence vers la valeur) transportée (fichier, hash, info)

REbus

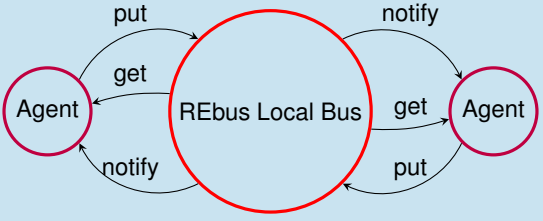
Protocole

- protocole du bus indépendant de son implémentation
- implémentés pour l'instant
  - local bus
  - REbus over DBus ($\Longrightarrow$ peut être réparti sur plusieurs machines)

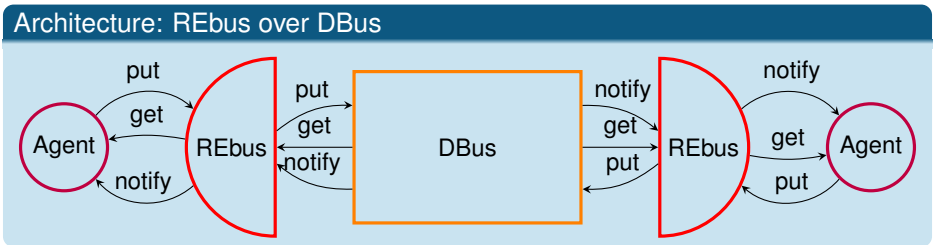
$\Longrightarrow$ implémentation des agents indépendante de l'implémentation du bus

REbus

Architecture: REbus Local Bus



REbus


Architecture: REbus over DBus
Agent
put
get
notify
REbus
put
get
notify
DBus
notify
get
put
REbus
notify
get
put
Agent

REbus

Utilisations envisagées / espérées

- Interfaçage rapide entre outils hétérogènes
- Usage collaboratif d'outils d'analyse
- Alternative à VirusTotal
- Classification de malwares