Secure your application with Artichokes

Casey Schaufler
Tomasz Świerczek

TIZEN DEVELOPER CONFERENCE 2014 SAN FRANCISCO
A word about our vegetable

• Artichoke in English
• Karczoch in Polish
• Cynara in Latin
The ones we didn’t use

- Polkit

- Polecat
What problem are we solving?

- Access control
- Arbitrary applications
- Abstract resources
What is Cynara?

- A library
- A dedicated service
- A policy DB
What does the application have to do?

- Application manifest
- List of privileges
- Smack label assigned by the installer
What about run time?

• Nothing
• We don’t trust applications
Credentials identify the application

- Smack label
What does the server have to do?

• Know its privileges
• Get credentials
• Call APIs
Cynara APIs

• 2 parts
  • Checking privilege
  • Registering applications data
• Synchronous API first
  • Need for asynchronous agreed, will be provided later
Cynara APIs for services

- Checking privilege – cynara-client
  - `initialize()` & `finalize()`
    - Configurable: socket name, client cache size, …
  - `cynara_check()` with `args`:
    - Application id
    - Applications session id
    - User id
    - Privilege requested
  - Result: `SUCCESS` or `ACCESS_DENIED`
Cynara APIs for policy setup

- cynara-admin library
  - Registering applications privileges
  - Registering extensions to policy
    - possible UI popups
Cynara performance

- Cynara good
  - < 10 ms for Yes/No DB query
  - Can be optimized with client-side cache

- Polkit bad
  - > 30 ms for Yes/No DB query
  - Linear increase with # of rules
    - Javascript & XML policy DB
Cynara future directions

- **Current state – alpha working**
  - cynara-client library operational
  - No dedicated cynara service yet

- **Roadmap**
  - Dedicated process – EOF June
  - cynara-admin – EOF June
  - cynara-client cache – EOF July
  - Moving to github – EOF July
  - Async client API – EOF August
  - Extensions – EOF August
Thank you