AppCLSM

A Linux kernel security module to implement application oriented access controls

Presented by James Johnson
Computing Showcase
23 May 2016

AppCL LSM

A Linux kernel security module to implement application oriented access controls

About Me

AppCL LSM

A Linux kernel security module to implement application oriented access controls

James Johnson

Graduating from Leeds Beckett University

BSc (Hons) Computer Forensics and Security

Developed AppCL LSM as my final year project

I like motorbikes

AppCL LSM

A Linux kernel security module to implement application oriented access controls

What am I talking about?

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Access Control Lists (ACL)
Program-based Access Control List (PACL)

User oriented, Application oriented

Linux Security Module (LSM) Framework
Extended Attributes

AppCLLSM

A Linux kernel security module to implement application oriented access controls

AppCLLSM

appclpy

AppCL LSM

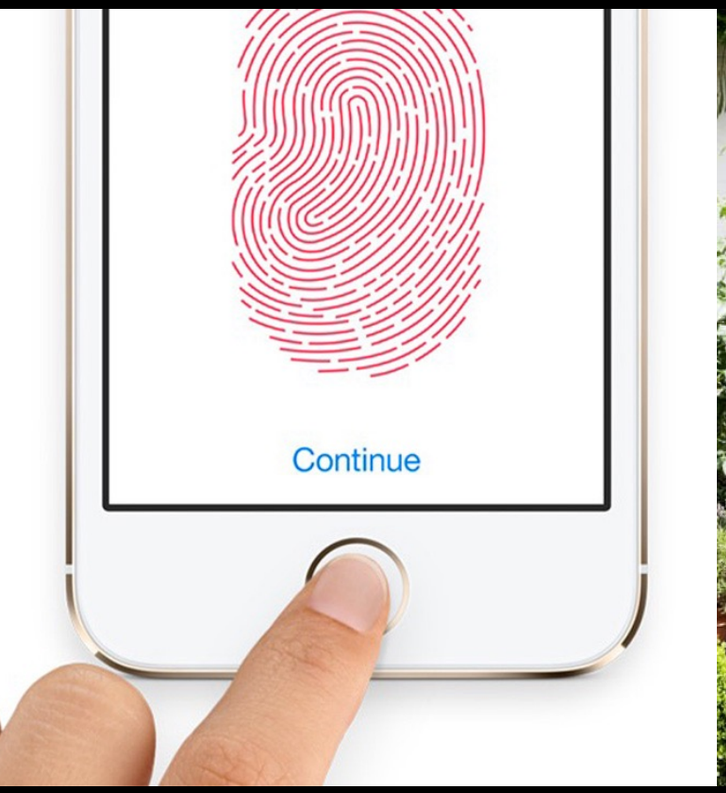
A Linux kernel security module to implement application oriented access controls

What is ‘Access Control’?

AppCL LSM

A Linux kernel security module to implement application oriented access controls

“Access Control: Is a set of controls to restrict access to certain resources.”



AppCL LSM

A Linux kernel security module to implement application oriented access controls

Some acronyms …

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Access Control in Linux

Mandatory Access Control (MAC)
Type Enforcement (TE)
Role-based Access Control (RBAC)
Multi-level Security (MLS)
Discretionary Access Control (DAC)
Access Control Lists (ACL)
Program based Access Control List (PACL)

AppCL LSM

A Linux kernel security module to implement application oriented access controls

ACL

Define the access rights and permissions **users** have for an object.

Read/Write/Execute

PACL

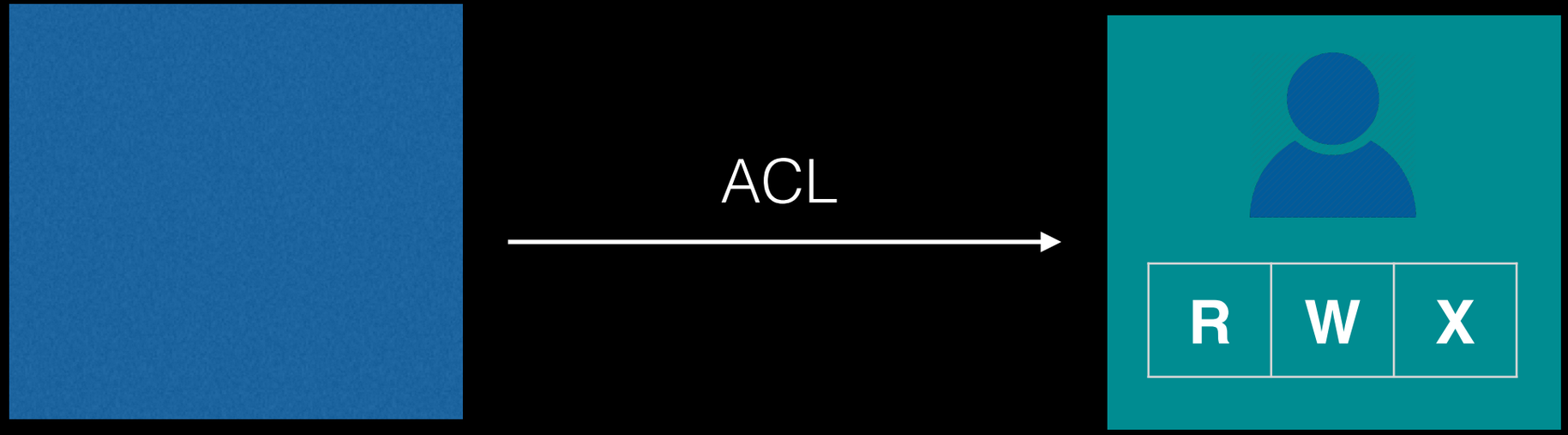
Define the access rights and permissions **applications** have for an object.

Read/Write/Execute

AppCL LSM

A Linux kernel security module to implement application oriented access controls

User oriented access control



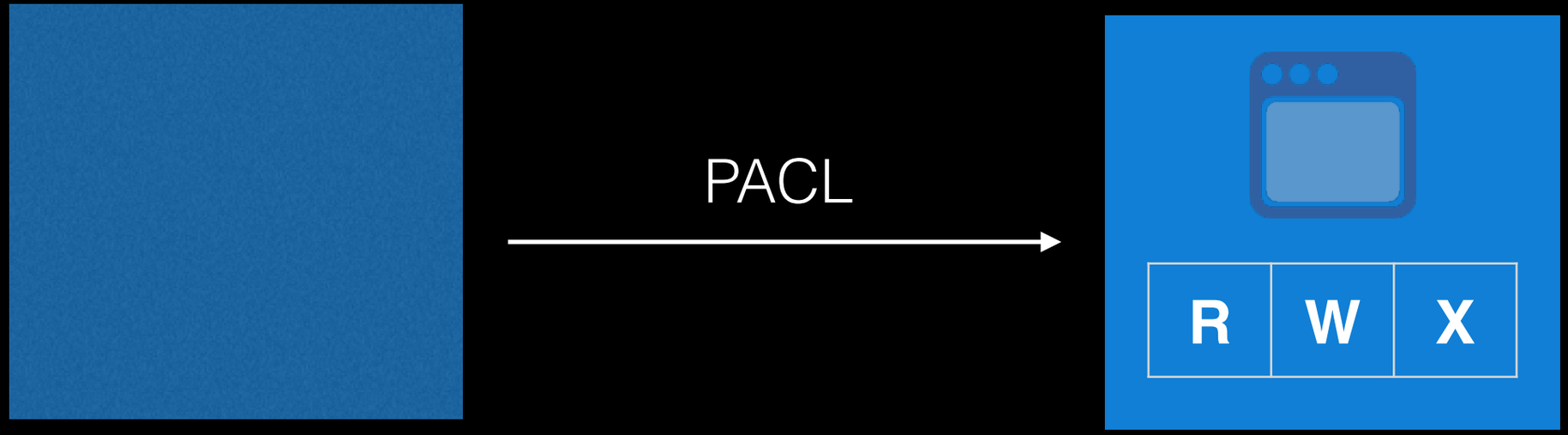
Object - Directory, file, etc

ACL - Access Control List

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Application oriented access control



Object - Directory, file, etc

PACL - Program based Access Control List

AppCL LSM

A Linux kernel security module to implement application oriented access controls

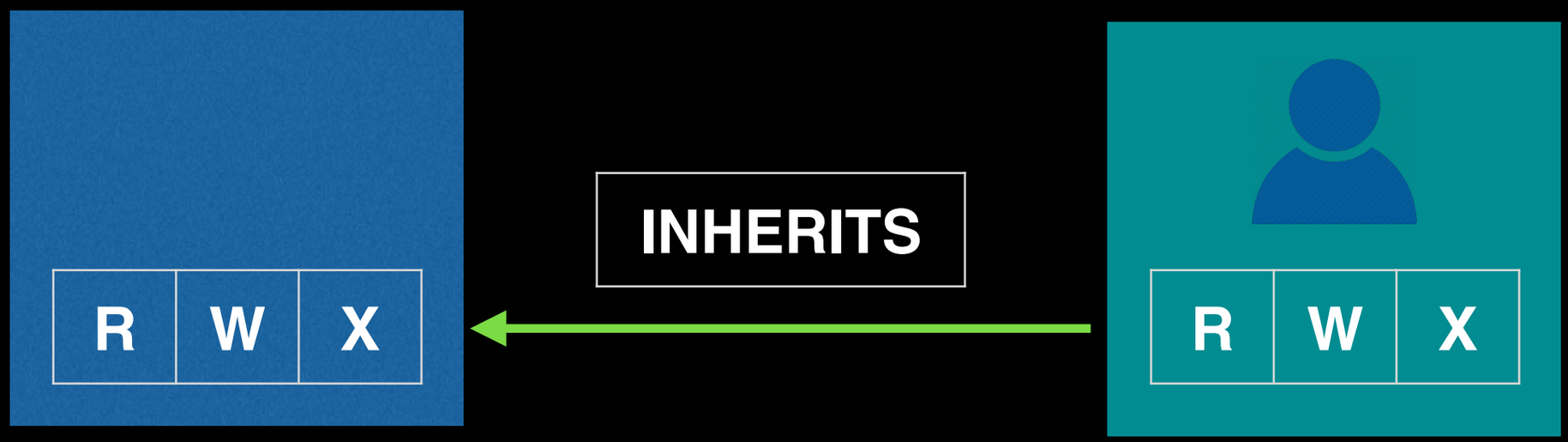
What’s the problem?

AppCL LSM

A Linux kernel security module to implement application oriented access controls

What's the problem?

Under a traditional Access Control List (ACL), Applications inherit the privileges of the user that runs the application.



Application - Calculator **User - someuser**

AppCL LSM

A Linux kernel security module to implement application oriented access controls

What's the problem?

Applications do not necessarily need the same permissions as the user running them grants.

Application specific threats

- Software vulnerabilities
- Malware

AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM

- Develop a Linux kernel security module that models a Program based Access Control List (PACL).
- Prevent applications inheriting the privileges of the user that runs them.
- Mimic the design and structure of a traditional ACL where possible.
- Provide a user friendly interface for managing the security policies.

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Implementing Application Oriented Access Control

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Implementing Application Oriented Access Control

- Linux Security Module (LSM) framework
- File system extended attributes

AppCL LSM

A Linux kernel security module to implement application oriented access controls

The Linux Security Module (LSM) framework

- LSM framework provides a general kernel framework to support security modules
- Primarily focused on supporting access control modules.
- By itself, the LSM framework does not provide any additional security.

AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM extended attributes

sudo apt-get **acl**	**ACL**	**setfacl** **getfacl**
sudo apt-get **attr**	**PACL**	**setfattr** **getfattr**

AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM extended attributes

The extended attribute value takes the following format:

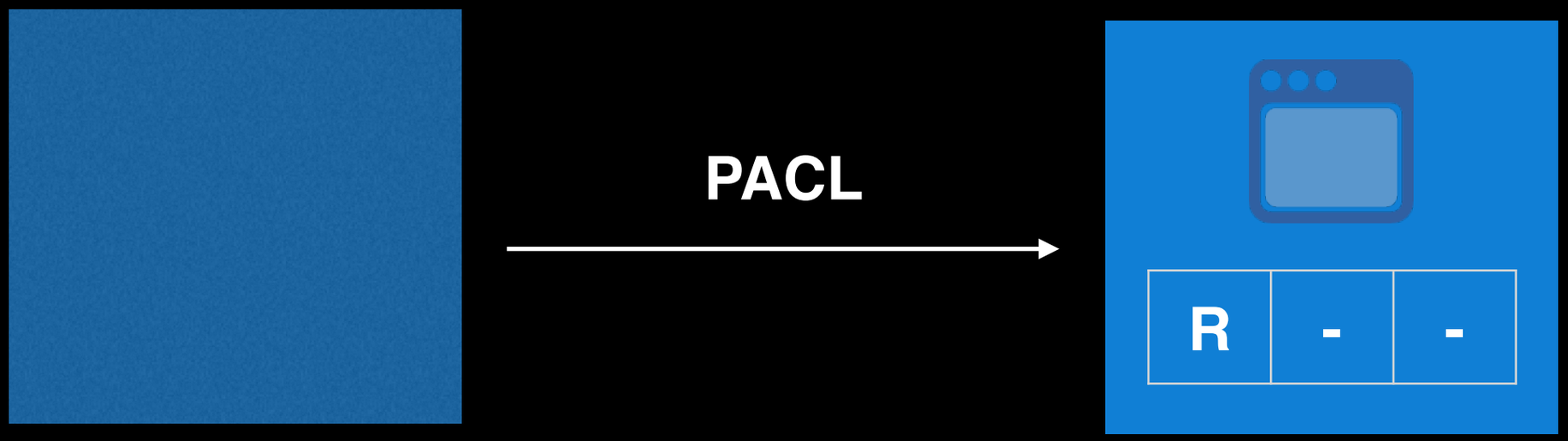
/path/to/app:perm;

AppCL LSM

A Linux kernel security module to implement application oriented access controls

The extended attribute value takes the following format:

/bin/nano:r;



File - /home/somefile

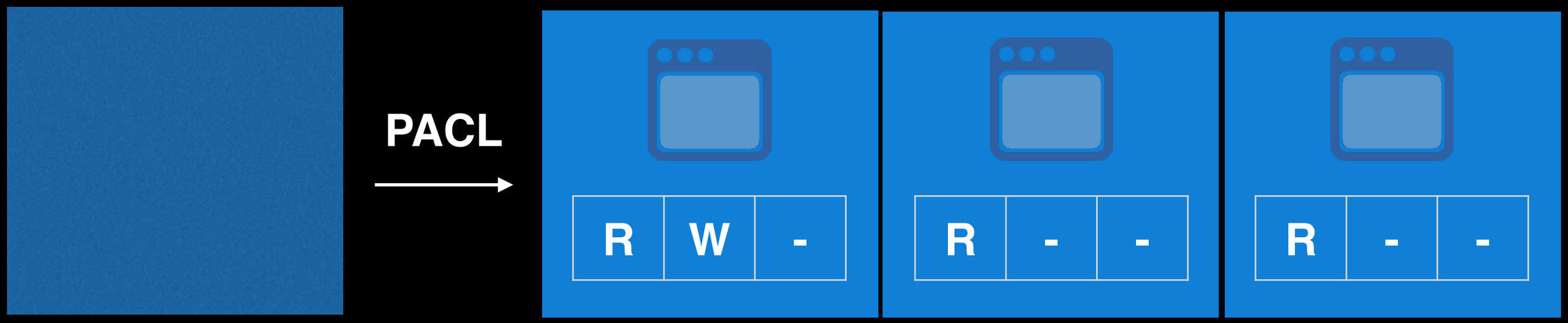
Application - nano

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Multiple permission entries can be set in the following format:

/bin/nano:rw;/bin/less:r;/bin/cat:r;



AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM extended attributes - default behaviour

Blacklisting

Default ALLOW

VS

Whitelisting

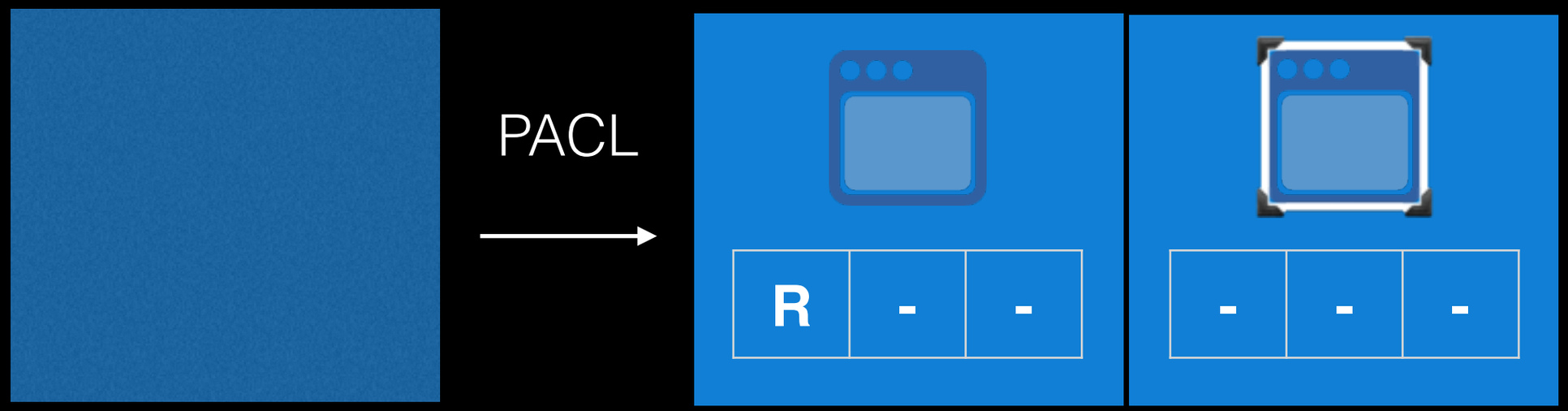
Default DENY

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Set the default DENY behaviour with the deny attribute *[deny:-;]*:

/bin/nano:r;deny:-;



File - /home/somefile

App - nano

DENY ALL

AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM

- Develop a Linux kernel security module that models a Program based Access Control List (PACL).
- Prevent applications inheriting the privileges of the user that runs them.
- Mimic the design and structure of a traditional ACL where possible.
- Provide a user friendly interface for managing the security policies.

AppCLSM

A Linux kernel security module to implement application oriented access controls

appclpy

- Provide a user friendly interface for managing the security policies.

AppCL LSM

A Linux kernel security module to implement application oriented access controls

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Conclusion

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Access Control Lists (ACL)
Program-based Access Control List (PACL)

User oriented, Application oriented

Linux Security Module (LSM) Framework
Extended Attributes

AppCLLSM

A Linux kernel security module to implement application oriented access controls

AppCLLSM

appclpy

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Questions?

AppCL LSM

A Linux kernel security module to implement application oriented access controls

Thank you!

AppCLSM

A Linux kernel security module to implement application oriented access controls

Presented by James Johnson
Computing Showcase
23 May 2016