It May Be Simple
But How Is It Useful
Smack Me Now!

Michael Demeter
Casey Schaufler
Smack Me Now
Simplified Mandatory Access Control Kernel

- Mainline Linux since 2008
- Standard in Tizen
Basic Rule

- What’s mine is mine
- What’s yours is yours
“Everything Should Be Made as Simple as Possible, But Not Simpler”
Isolation Is Easy

Sharing Is Hard
How Does An Application Get Its Smack Label?

• /proc/self/attr/current
• SMACK64EXEC
Privilege

- Linux capabilities
- cap_mac_override
- cap_mac_admin
Domains

• All processes labeled Mike
• All files labeled Mike
Access Rules

- Process Smack label
- Smack label on the thing
- What kind of access
How Files Work

- You can’t change what you can’t see
- Read or execute access to look and see
- Write or append access to change
How Communications Work

- Messages need write access
You have the ingredients
Domain Granularity
When Is Simple Too Simple
A Case Study

- Simplify Installation
- Weave a tangled web
- 600+ Packages
- 20,000+ access rules
- Attack surface increased

Do you believe the software contained in these packages is defect free?????
“You security people are insane!”
Finally …
TIZEN™
DEVELOPER CONFERENCE
2013
SAN FRANCISCO