

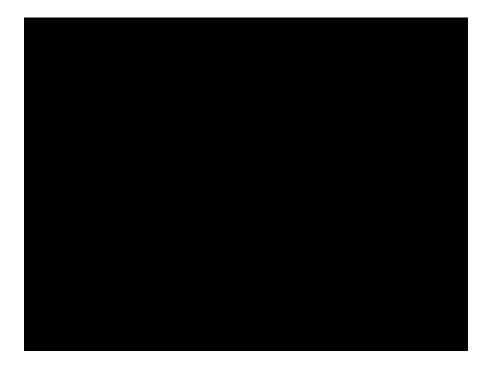
It May Be Simple
But How Is It Useful
Smack Me Now!

Michael Demeter Casey Schaufler



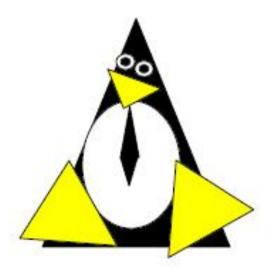
SAN FRANCISCO

### **Smack Me Now**



### **Simplified Mandatory Access Control Kernel**

- Mainline Linux since 2008
- Standard in Tizen

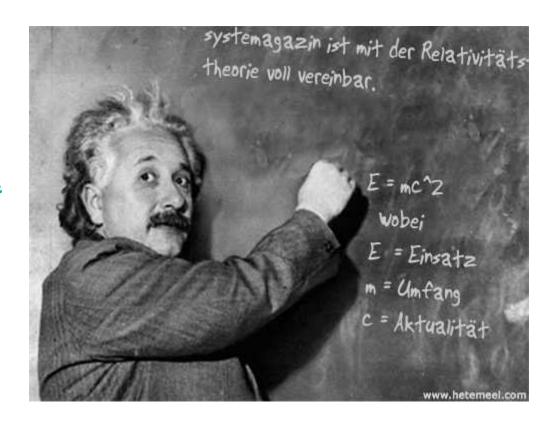


#### **Basic Rule**

- What's mine is mine
- What's yours is yours



"Everything Should Be Made as Simple as Possible, But Not Simpler"





## **Isolation Is Easy**









### **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

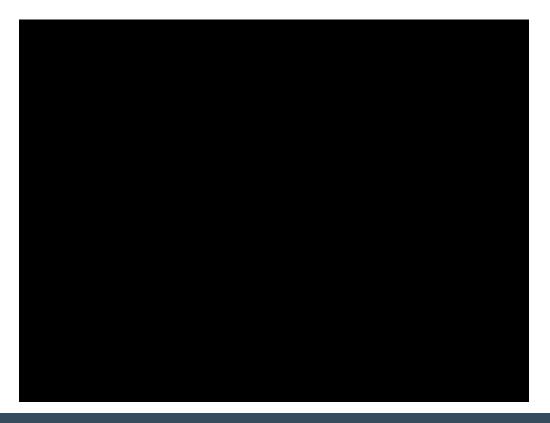


### **How Communications Work**

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?????

x2000/00/
url-playid-dynam
url-installer
url .
uerldelesk
wifi_dirret_bases
urthil2-rft
ant-printer-Dericke
as blarfacile a
aginagrainuri M
The state of the s
Harring
Hambererer Irlephang franchisch
agalen::ase_isterari
applementary
andre -
agaraneri::atto:Danter
manny like
airtala -
all-arrer
starter
aglfa -
anarlaard-arraiar
arasar-fraurusch
arasrily-arrare
parkerraine
polaredia
paure_manger
hydracerren
things provided the second
phymyr-installer
physical and the second
physical restriction of the state of the sta
espinalatter ///////////////////////////////////
tials/// / ////////////////////////////
erg.liere.seleur
erg.liere.nidre-player
erg.liere.asbragapapa
erg.liere.liebrleeli-/quegage/
erg.liere.laskmar
erg.liere.ordling
erg.liera.estei
erg.liere.gainbp.es////////////
erg.liere.pulsek // /// //
eraliseashar // /// ////
eralises.orleanife /// /////
erg.liere.mg6ite
erg.liere.main-plater
eraliera.erasay///////////////////////////////////
/ / / / / / / / / / / / / / / / / / /
arg.liara.mranyherra///////////////////////////////////
erg.liere.urus
arq.liara.uraa-ghreen arq.liara.uraa arq.liara.laahaarera
englisen.energenergenergenergenergenergenergen
arg.liare.areas arg.liare.areas arg.liare.lashaarera arg.liare.india.lar arg.liare.india.lar
arg.lire.urus arg.lire.larkarera arg.lire.larkarera arg.lire.idisaler arg.lire.urus arg.lire.urus
arglieramanykere arglierahakaren arglierahakaren arglierahitaka arglierangerirak arglieragilera arglieragilera
orgilira.orgi orgilira.orgi orgilira.orgi orgilira.orgilira orgilira.orgilira orgilira.orgilira orgilira.orgilira orgilira.orgilira
or, live-associates or, live-labores or, live-labores or, live-labores or, live-labores or, live-aboutes or, live-aboutes or, live-aboutes
artikaransuparas artikaransu artikaransu artikaransuparas artikaransul artikarans
or, live associates or, live associates or, live a listance or, live a listance or, live a listance or, live a live a live a or, live a live a or, live a live a live a live a live a or, live a live a or, live a li
artitaramenteres artitarament
or, live associates or, live associates or, live a listance or, live a listance or, live a listance or, live a live a live a or, live a live a or, live a live a live a live a live a or, live a live a or, live a li

```
erg.liere.mgfile
erg.liere.phoer
erg.liere.esslasle
erg.liere.esslade-sirure
erg.liere.esleer
erg.liere.eidre-plager
erg.liere.asb-agapapap
erg.liere.liebrreeli-agapapap
ere.liere.laskeer
erg.liere.emarlerarek
erg.liere.erlling
erg.liere.eal-si
erg.liere.quiebparel
ere.liere.sulesk
eraliera.erleanen
erg.liere.masis-plager
erg.liere.mranage
erediare.eres
erediere.eres
eralliara.laskaarres
erq.liere.iediealer
erg.liere.imagr:sirurr
erq.liere.qallerq
erg.liere.reail
org.liara.draglask
erg.liere.deuelead-marger
erq.liere.dala-presider-urhapp-elase
org.liora.dala-prosfere-ulaur
erg.liere.dala-predider-manler
erg.liere.eleek
erg.liere.sies
erq.liere.eamera-app
erg.liere.eall
erg.liere.ealredar
erg.liere.ealestater
erg.liere.bl-agapapap
erg.liere.breuerr
era,liara,blarlaulb-share-si
erelliere.apprerleeler
```

gereer-elerage rusal

"You security people are insane!"



# Finally ...





