Pledge(2)
En sandbox för OpenBSD

icepic@deadzoft.org

Olika metoder för inkapsling:

Olika metoder för inkapsling:

- Virtualisering (VMware, Xen, KVM, Shapeshifter)
- Komplett emulering (qemu, bochs, PCtask)
- Bytecode VM (JVM, .Net, LLVM, ruby, perl, lua)
- chroot/jail/UML/zones/ldomains

Alla typer av inkapsling ger olika typer av säkerhet

Alla typer av inkapsling ger olika typer av säkerhet

- En hackad gäst är fortf. en hackad maskin
- En applikation i en bytecode runtime-miljö kan i princip allt som runtime:n nånsin kommer kunna

Alla typer av inkapsling ger olika typer av säkerhet

OS:et kan hjälpa till med ASLR, W^X, random malloc(2)s, random ordning på lib-länkning, osv

Alla typer av inkapsling ger olika typer av säkerhet

Man måste begränsa vilka
OS-anrop som ditt program
(inkl. alla libs som den länkat mot)
kan utföra

Förr eller senare
måste man gå ner till
en enskild applikation
och säkra upp den

Vad finns det för tekniker för att sandboxa applikationer?

SELinux

AppArmor

Seccomp

Capsicum

Systrace

SELinux

AppArmor

Seccomp

Capsicum

Systrace

SELinux

AppArmor

Seccomp

Capsicum

Systrace

SELinux

AppArmor

Seccomp

Capsicum

Systrace

SELinux

AppArmor

Seccomp

Capsicum

Systrace

Pledge

Pledge

Kommer lite ur metodiken

“Privilege separation”

Pledge

Kommer lite ur metodiken
“Privilege separation”

Växte fram efter att ha priv-sep:at
file(1) och tcpdump(8)

Pledge

Inline:at i sourcen till ditt program

Pledge

Inline:at i sourcen till ditt program

Gör att du kan ändra vid rätt tillfälle
beroende på i vilket state ditt program är

Pledge

Inline:at i sourcen till ditt program

Gör att du kan ändra vid rätt tillfälle
beroende på i vilket state ditt program är

Nästan alla program har samma struktur

Pledge

Init - Allokera/öppna resurser, sockets, filer

Mainloop - Få eller inga nya resurser skaffas

Pledge

Init - Allokera/öppna resurser, sockets, filer
<- perfekt plats att stoppa nyallokering
Mainloop - Få eller inga nya resurser skaffas

Pledge

Simpla fall: (mkdir)

```
main(int argc, char *argv[])
{
        int ch;

 +      if (pledge("stdio cpath rpath wpath fattr”,
NULL)==-1)
 +              err(1, "pledge");
```

Pledge

Mer komplicerade exempel: doas (typ sudo)

```
+if (pledge("stdio rpath getpw proc exec id", NULL) == -1)

+if (pledge("stdio rpath getpw exec id", NULL) == -1)

+if (pledge("stdio rpath id exec", NULL) == -1)

+if (pledge("stdio rpath exec", NULL) == -1)

+if (pledge("stdio exec", NULL) == -1)
```

Pledge

Parametrar till pledge(2):
Textsträng väljer grupper av anrop
att tillåta från nu och framöver

Kan anropas mer än en gång,
men bara med färre rättigheter
än vad man hade innan

Pledge

Olika typer av pledge man kan be om:

Pledge

Olika typer av pledge man kan be om:

stdio: - Allt som krävs för output till konsol eller fil

Pledge

Olika typer av pledge man kan be om:

stdio: - Allt som krävs för output till konsol eller fil

rpath / wpath: Allt som krävs för att läsa eller skriva till delar av filsystemet

Pledge

Olika typer av pledge man kan be om:

stdio: - Allt som krävs för output till konsol eller fil

rpath / wpath: Allt som krävs för att läsa eller skriva till delar av filsystemet

inet: Allt som krävs för att prata nätverk

Pledge

Olika typer av pledge man kan be om:

stdio: - Allt som krävs för output till konsol eller fil

rpath / wpath: Allt som krävs för att läsa eller skriva till delar av filsystemet

inet: Allt som krävs för att prata nätverk

dns: Allt som krävs för att slå upp hostnamn

Pledge

Olika typer av pledge man kan be om:

stdio: - Allt som krävs för output till konsol eller fil

rpath / wpath: Allt som krävs för att läsa eller skriva till delar av filsystemet

inet: Allt som krävs för att prata nätverk

dns: Allt som krävs för att slå upp hostnamn

proc: Allt som krävs för fork(2), kill(2) osv

Pledge

Status idag

Pledge

Cirka 400 av 600 program täcks
av pledge i OpenBSD idag

Pledge

Enbart ett fåtal av de
3e-parts-programmen (ports)
som kan installeras på OpenBSD
har pledge. Men bland de som
har det är bzip2/xz osv som är
involverade i massor av hantering
av “untrusted data”