

# Mach security

Vincenzo Iozzo

snagg@openssl.it

SMAU 2007, 20/10/2007

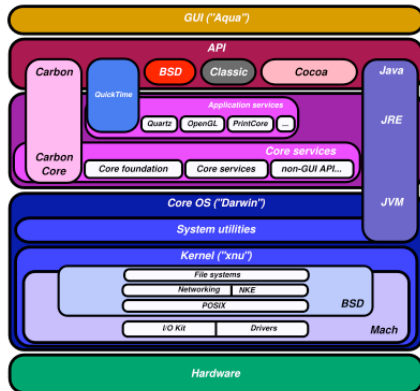
- Mach 3.0: Virtual Memory, IPC, Scheduling
- 4.4BSD: Accessi file, Sicurezza, Processi

- Microkernel sviluppato dalla Carnegie Mellon University
- Si base sullo scambio dei messaggi
- Gestisce le primitive della memoria e dello scheduling

- Task
- Thread
- Port
- Port Set
- Message
- Memory Object

- I permessi sono gestiti dai privilegi sulle porte mach
- Non fa check sull'autenticazione
- La policy di sicurezza in XNU è gestita a livello BSD

# Sguardo di insieme



- **PTRACE\_PEEKTEXT, PTRACE\_PEEKDATA, PTRACE\_POKETEXT, PTRACE\_POKEDATA** sono sostituite dalle primitive per la gestione di memory object di Mach (vm\_alloc, vm\_write, vm\_read)
- **PTRACE\_GETREGS, PTRACE\_SETREGS** sono sostituite da thread\_get\_state e thread\_set\_state

# Codice

- Mach può bypassare alcuni sistemi di sicurezza BSD
- Se due task appartengono ad uno stesso utente, i privilegi sulla porta sono garantiti
- Se una zona della memoria appartiene al kernel, l'utente root da userspace è in grado di scrivere in quella zona di memoria

- I processi che girano sotto chroot appartengono ad uno stesso utente che sta fuori la jail
- Dall'interno della jail è possibile “agganciare” dei processi all'esterno e injectare codice nella loro memoria per rompere chroot

# Codice

# Get Out!

```
hesiod:/tmp snag$ sudo chroot jail/  
bash-2.05b# ./exp 611  
bash-2.05b# telnet localhost 4444  
cd /Users/snagg  
pwd  
/Users/snagg
```

- Creare lo shellcode con il codice precedente
- Sfruttare vulnerabilita' di un service remoto dentro chroot

- Sysctl da delle informazioni sul kernel, nella maggior parte delle volte modificabili solo a kernel space
- I securelevel del kernel sono dei livelli di sicurezza “predefiniti” che possono essere aumentati a userspace ma non diminuiti
- Attraverso Mach possibile cambiare i livelli di sicurezza da userspace

```
nm /mach_kernel | grep securelevel  
004bcf00 S _securelevel
```

# Codice

```
hesiod:/tmp snag$ sudo sysctl -w kern.securelevel=0
Password:
kern.securelevel:  Operation not permitted
hesiod:/tmp snag$ sudo ./slevel -1
hesiod:/tmp snag$ sysctl -a | grep secure
kern.securelevel = -1
```

- Rootkit
- Code injection
- Shellcode

Grazie per la cortese attenzione