



Art of Embedded Linux

CIH <Software Magician>
集嘉通訊 總經理室 專屬 主任工程師

Embedded Linux Memory Mapping



WinCE Memory Mapping

0000-0000	<i>Slot 0</i>	<i>Current Process</i>
0200-0000		
0400-0000	<i>Slot 1</i>	<i>XIP Dlls</i>
0600-0000	<i>Slot 2</i>	<i>Process 2(filesys.exe)</i>
0800-0000	<i>Slot 3</i>	<i>Process 3(device.exe)</i>
0A00-0000		
0C00-0000	<i>Slot 4</i>	<i>Process 4</i>
	
4000-0000		
4200-0000	<i>Slot 32</i>	<i>Process 32</i>
	<i>Share Memory</i>	
8000-0000	<i>Kernel space</i>	
FFFF-FFFF		<i>Process 1(NK.exe)</i>

- *User space*以及*Kernel space Memory Mapping*全部攪在4GB虛擬記憶體(大鍋菜!?)
- 系統最多只能有32個*Process*
- 每一個*Process*最大記憶體空間是32MB
- *User Process*之間，絕對不會互相毀掉彼此(除非使用*WriteProcessMemory*或是*SetProcPermissions*等函式)
- *User Process*隨便就能毀掉*Kernel*(可以用*SetKmode*提昇自己權限，變成*kernel*權限)
- *User/Kernel API*完全混在一起(真是水乳交融啊)
- *User*以及*Kernel*權限看起來有獨立，其實是騙小孩的!!
`GetModuleFileName(NULL, (WCHAR *)0xffff0000, 256);`
- 系統的安全穩定性!?!有這一回事嗎!?!

- *User space*以及*Kernel space Memory Mapping*清楚分明
- *User Process*之間，絕對不會互相毀掉彼此
(除非使用root權限去執行ptrace等函式)
- *User Process*絕不可能毀掉*Kernel*
- *User/Kernel API*完全獨立(*User*只能使用*User API*、*Kernel*只能只用*Kernel API*)
- *User*以及*Kernel*權限獨立分開
- 系統絕對性安全

- 要CoCo (錢)
 - 整合性非常好 (微軟都幫你做好了)
 - PDA、Phone、多媒體影音產品
 - Support的CPU非常有限 (以x86、ARM的Support最最完整)
 - 系統安全穩定性!?
- 嗯~不跑任何程式、不上網，就真的非常安全穩定!!我說真的!!

- 幾乎不用**CoCo**，所有東西幾乎有**Open Source Code**可以拿過來用
- 整合性非常不好，什麼東西整合都要靠自己
- 在**PDA**、**Phone**、多媒體影音產品慘兮兮
- 在網通產品是最大量採用的**OS**系統
- **Support**的**CPU**異常多 (**x86**、**ARM**、**PPC**、**m68k**、**MIPS**、**SH**等等等等)
- 系統安全穩定性，非常非常穩定安全!!



Thank You

***CIH <Software Magician>
Phone: 0928-157-600
E-mail: IamCIH@gmail.com***