

linux em sistemas embebidos

linux em sistemas embebidos

Rui Covelo & Pedro Venda

linux em sistemas embebidos

- Trabalho Final de Curso

“Segurança no Acesso a Sistemas Embebidos”

carregamento remoto de um sistema operativo

comunicação segura

protecção contra intrusão

confiança no funcionamento

recursos limitados

linux em sistemas embebidos

- sistema embebido
- linux embebido
 - panorama actual
- Bullet Linux
 - objectivo
 - solução proposta
 - *“making of”*
 - demonstração
- segurança no carregamento remoto de um sistema operativo

sistema embebido

o que é?

- “computador” com função específica
- conjunto limitado de funções
- utilização integrada em sistemas mais complexos
- recursos limitados... ou então não...

sistema embebido

importância

- papel importante no quotidiano e na indústria
 - *handhelds* (telemóveis, PDAs, etc.)
 - sistemas de monitorização
 - sistemas de controlo
 - aparelhos de comunicação
 - electrodomésticos
- futuro próximo
 - domótica

linux embebido

- fiabilidade
- escalabilidade
- flexibilidade & modularidade
 - versatilidade das distribuições
 - kernel composto por diversos módulos
 - possibilidade compilar o kernel apenas com os modulos necessários à aplicação

linux embebido

- *software* livre

... given enough eyes, all bugs are shallow ...

Linus Torvalds

- código disponível para ser consultado e alterado
- adaptação do *kernel* ao mais variado *hardware*
- baixo custo
- evolução de encontro às necessidades académicas e do mercado

linux embebido

tecnologias existentes

- várias distribuições existentes
 - distribuições apostam nos *handhelds*
 - versões otimizadas para equipamentos de rede
 - versões otimizadas para uso de *hardware* mais antigo

AMSEL

Advanced Modular Secure Embedded Linux

- sistemas embebidos com requisitos elevados de segurança
 - protecção de memória contra *stack smashing*
 - impossibilidade de execução de código na pilha
 - sistema de separação de privilégios de serviços
- extensões de tempo real
 - baixa latência do kernel
 - preempção

uClinux

- adaptação do linux (2.4) para sistemas sem MMU
 - redução da necessidade de recursos
 - não existe protecção de memória entre processos
 - não suporta múltiplos processos em execução

Linksys NSLU



Network Storage Link for USB

- aparelho de rede para armazenamento de dados
- acesso via SMB (*server message block*)
- versão comercial de linux
- possui:
 - controladora USB
 - 32MB de memória
 - processador de 266, 400 ou 533MHz (Intel IXP - ARM)
 - 2 interfaces USB para ligação de discos
 - 1 interface *ethernet*

Linksys WRT54G



Wireless-G Broadband Router

- wireless router
- suporte para IEEE802.11b/g
- switch ethernet de 5 portas
- versão comercial do linux
- utilização de outras aplicações *open-source*
- possui:
 - 16MB memória RAM
 - 4MB memória *flash*
 - CPU 200MHz MIPS
 - 5 portas *ethernet* 10/100Mb

Bullet Linux

- distribuição minimalista com fins académicos
 - estudo do linux em sistemas com recursos limitados
 - funcionamento possível em:
 - arquitectura 486
 - 8MB RAM
 - sistema completo funcional com <1.44MB
 - suporte de interfaces de rede *ethernet*
 - pilha de protocolos TCP/IP

Bullet Linux

- linux kernel 2.6

- significativamente melhor do que a versão 2.4
- preemptividade nas chamadas de sistema
- *scheduler* com complexidade $O(1)$
- muito mais escalável (menor latência)
 - sistemas embebidos
 - supercomputadores
- suporte para novas arquitecturas incluindo processadores em MMU
 - Motorola 68000
 - Hitachi H8/300
 - NEC v850

Melhor desempenho em ambientes de tempo real MAS não dá garantias

Bullet Linux

- biblioteca de sistema uClibc (Erik Andersen)
 - biblioteca desenvolvida tendo em vista ambientes com poucos recursos
 - reescrita com objectivo de optimização do tamanho do código produzido
 - modularização e compartimentação de funcionalidades para configurações adequadas ao ambiente alvo
 - libc vs uClibc
 - 1300 KB vs 300 KB

Bullet Linux

- *busybox* (Erik Andersen)
 - condensa num só binário as funcionalidades de diversas ferramentas
 - init, ls, ifconfig, ash, mount, etc...
 - otimização e reaproveitamento de código binário
 - ferramentas com limitações de opções
 - sistema de configuração em “*curses*”

“*making of*”

- buildroot (Erik Andersen)
 - criação de ambiente de desenvolvimento
 - *cross-compiler* (gcc), *linker* (ld), *assembler* (as)
 - libc (uClibc)
 - ferramentas de sistema (busybox)
- gera *filesystem*
 - *initrd* (ferramentas de sistema apenas)
 - ambiente de desenvolvimento (ferramentas de sistema e de desenvolvimento)
- sistema de configuração em “*curses*”

“making of”

- sistemas de configuração em “curses”
 - make menuconfig

Toolchain Options

Arrow keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> selects a feature, while <N> will exclude a feature. Press <Esc><Esc> to exit, <?> for Help. Legend: [*] feature is selected [] feature is excluded

```
~(-)
Kernel Headers (Linux 2.6.11 kernel headers) --->
--- uClibc Options
[*] Use the daily snapshot of uClibc?
[ ] Enable locale/gettext/i18n support?
--- Binutils Options
  Binutils Version (binutils 2.15.91.0.2) --->
--- Gcc Options
  CC compiler Version (gcc 3.4.2) --->
  (0) Additional gcc options
  [*] Build/install c++ compiler and libstdc++?
```

!(+)

<Select> < Exit > < Help >

Desktop Configuration

Arrow keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are hotkeys. Pressing <Y> selects a feature, while <N> will exclude a feature. Press <Esc><Esc> to exit, <?> for Help. Legend: [*] feature is selected [] feature is excluded

```
|| General Configuration --->
  Build Options --->
  Installation Options --->
  Archival Utilities --->
  Coreutils --->
  Console Utilities --->
  Debian Utilities --->
  Editors --->
  Finding Utilities --->
  Init Utilities --->
```

!(+)

<Select> < Exit > < Help >

“making of”

- sistemas de configuração em “curses”
 - make menuconfig

```
Linux Kernel v2.6.11 Configuration

Ethernet (10 or 100Mb/s)
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </>
for Search. Legend: [*] built-in [ ] excluded <M> module <>
^(-)
<> etherExpressPro/100 support (eepro100, original Becker driver)
<> Intel(R) PRO/100+ support
<> Mylon MTD-8xx PCI Ethernet support
<> National Semiconductor DP8381x series PCI Ethernet support
<> PCI NE2000 and clones support (see help)
<> RealTek RTL-8139 C+ PCI Fast Ethernet Adapter support (EXPERIME
<> RealTek RTL-8139 PCI Fast Ethernet Adapter support
<> SiS 900/7016 PCI Fast Ethernet Adapter support
<> TMC EtherPower II
<> Sundance Alta support
+(-)

<Select> <Exit> <Help>
```

```
Linux Kernel v2.6.11 Configuration

Device Drivers
Arrow keys navigate the menu. <Enter> selects submenus --->.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </>
for Search. Legend: [*] built-in [ ] excluded <M> module <>
^(-)
Character devices --->
I2C support --->
Dallas's 1-wire bus --->
Misc devices --->
Multimedia devices --->
Graphics support --->
|| Sound --->
USB support --->
MMC/SD Card support --->
InfiniBand support --->

<Select> <Exit> <Help>
```

processo de arranque

- BIOS
 - vários dispositivos podem arrancar
 - *floppy*
 - discos
 - placa de rede (*takeover* do processo de arranque)
- *bootloader (floppy, discos)*
 - *syslinux, lilo, grub*

arranque via ethernet

- *etherboot* (PROM, floppy)
 - DHCP
 - TFTP
 - *kernel* + *initrd* em “envelope” ELF
- PXE (*Pre boot eXecuting Environment*)
 - DHCP
 - TFTP
 - *bootloader* (*pxelinux*, *pxegrub*)
 - *kernel*, *initrd* (ou qualquer coisa que o bootloader entenda)

Bullet Linux 0.11f

- arranque a partir de uma disquete com 3 componentes essenciais
 - *kernel*
 - *bootloader (syslinux)*
 - imagem do sistema de ficheiros inicial (*initrd*) para instalação em *ramdisk*
- funcionalidade
 - suporte para periféricos de entrada
 - suporte para monitor VGA
 - drivers para vários interfaces de rede
 - pilha de protocolos TCP/IP

Bullet Linux 0.11e

- arranque via rede *ethernet*
 - *etherboot*
 - *kernel* + imagem do sistema de ficheiros
 - “envelope” ELF (formato binário)
- funcionalidade
 - semelhante à versão 0.11
 - dispensa suporte de *floppy* drive

Bullet Linux 0.11n

- arranque via rede *ethernet*
 - *etherboot*
 - *kernel* em “envelope” ELF
 - *root filesystem* NFS
- maior funcionalidade
 - sistema de ficheiros encontra-se no servidor
 - desaparece a limitação de espaço
 - mais memória disponível (dispensa *initrd*)

demonstração

- arranque por *floppy*
 - Bullet Linux v0.11
- arranque por rede (PXE ou *etherboot* – o que funcionar...)
 - Bullet Linux v0.11e
- arranque por rede (PXE ou *etherboot*)
 - Bullet Linux v0.11n

ataque ao processo de carregamento remoto

- cenário 1 (DoS)
 - servidor de DHCP com gamas limitadas de endereços
 - MAC *spoofing*
 - ataque por esgotamento da gama de endereços do servidor de DHCP
- cenário 2 (DoS/ID *spoofing*)
 - servidor de DHCP com reservas por MAC
 - MAC *spoofing*
 - *usurpação* de identidade
 - obtenção de configuração e recursos dirigidos a um cliente legítimo

ataque ao processo de carregamento remoto

- cenário 3 (*ID spoofing*)
 - resposta a pedidos de DHCP feita por um servidor de DHCP intruso
 - disponibilização de recursos alterados (kernel, sistema operativo...)
- cenário 4 (*king of the world*)
 - *sniffing* de comunicação
 - utilização de combinação de ataques
 - obtenção de chaves de acesso
 - entrada não autorizada em clientes já em funcionamento
 - ...

FIM

Perguntas & Respostas

Contactos:

Pedro Venda: `pjlv@mega.ist.utl.pt`

`http://arrakis.dhis.org`

Rui Covelo: `rpfc@mega.ist.utl.pt`

`http://ruicovelo.2ya.com`