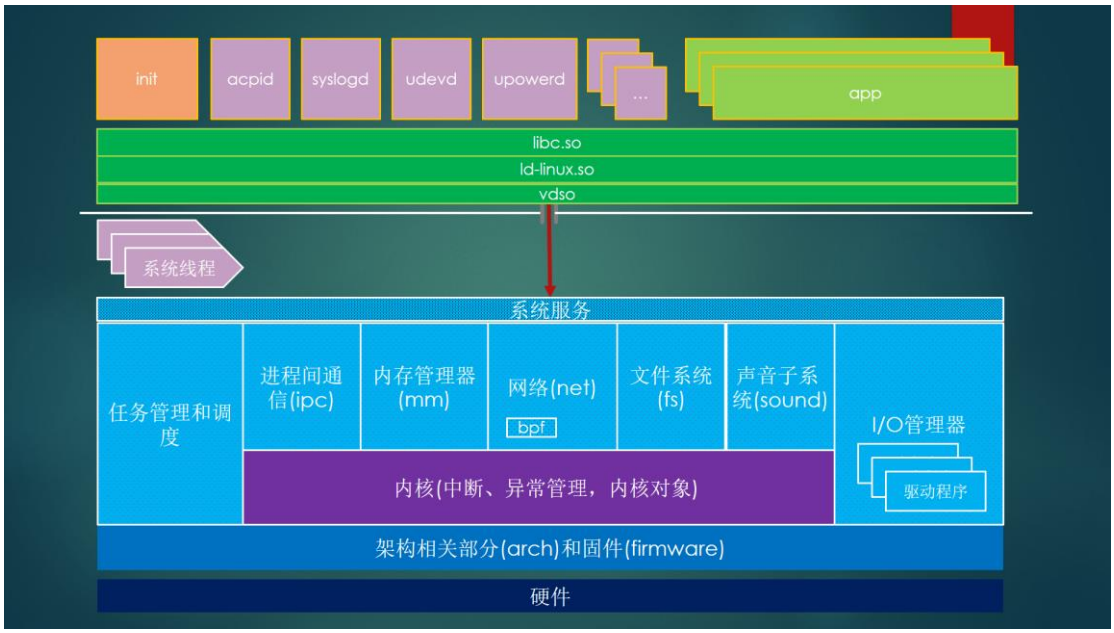
软件调试高级研习班 2018 上海站

LINUX 平台高级调试和优化

关于 LINUX 的资料浩如烟海，学习 LINUX 的途径也有很多，如何才能在比较短的时间里获得一个比较大的提升呢？《软件调试高级研习班》将与各位 LINUX 爱好者共同探索这个问题的最佳答案。本着生动有趣、理论与实践密切结合的原则，本研习班独辟蹊径，使用调试之剑披荆斩棘，带你闯荡纷繁复杂的 LINUX 世界。以格物精神，钻研代码，深挖 LINUX 系统的核心机制，这一讲求得一理，下一讲再求得一理，步步推进。整个研习班，旨在实现三大目标：（一）深入理解 LINUX 操作系统的基础设施和核心机制；（二）学习开发 LINUX 程序（内核模块和应用程序）的工具和方法（三）学习 LINUX 平台上的调试工具和调试典型问题的方法。本研习班由《软件调试》和《格蠹汇编》的作者张银奎携手 INTEL 系 LINUX 高手程煜明博士共同担任教练。今年 4 月，本研习班曾在庐山秀峰成功举办，这一次移师上海，在上一届的基础上增加了实战内容，并适当增加深度。

时间：2018 年 9 月 21 日 - 9 月 23 日（周五-周日）
地点：上海
形式：实战演练、讲解和讨论点评
时间长度：3 天
培训对象：在 Linux 平台上从事开发或测试的软件工程师、项目带头人和技术经理
主办单位：高端调试网站、上海曜印网络科技有限公司

第一部分：LINUX 系统大局观 （1 小时）
要点：Linux 内核的早期版本，推动 Linux 发展的两股力量，GPL，Tainted，反面典型 Nvidia，解析内核源代码树， Linux 架构，ld（Loader），libc，重要的内核模块，Linux 的主要发行版本，Linux 的主要开发者，内核参数，内核文档和工具链（GCC）



第二部分：全面认识 GDB 之用户态调试（1.5 小时）

要点：为自由而生，Richard Stallman 传奇，GDB 诞生记，GDB 版本，GDB 的架构和工作原理，ptrace，命令类型，命令语法，常用命令，调试符号，DWARF，符号文件，下载 Ubuntu 的符号包和源代码，ELF 结构，readelf，寻找符号的方法，栈回溯（bt），软件断点、硬件断点，复杂的断点命令，控制线程

第三部分：应用程序崩溃和转储（1 小时）

要点：信号，信号处理器，信号屏蔽，使用 setjmp 和 longjmp 处理异常，Ubuntu 的错误报告机制， 使用 Python 脚本定制和收集更多信息

实战 1：使用 GDB 调试后台服务因段错误崩溃 （90 分钟）

Linux 下重要后台服务(Daemon)随机崩溃，深挖到底，竟然与 C 语言的规范有关，让你深刻认识 C 与 C++的一个大不同之处，感受著名的头文件陷阱；熟悉如下工具和主要技能：GDB，GCC，map，dmesg，调试 Linux 应用程序，反汇编，插入代码 JIT 调试；温习如下知识点：虚拟内存，分页机制，页表，缺页异常，段错误，空指针，AT&T 汇编和 Intel 汇编，调用规约

第四部分：CORE 转储和分析（1 小时）

要点：Core 机制，配置产生 core 文件，使用 gdb 分析 core 文件，加载符号，手工回溯栈，案例讨论，分析 Core 转储的最佳实践

第五部分：全面认识 GDB 之内核态调试（1.5 小时）

要点：Linus 对内核调试的态度，艰难推进，KDB 与 KGDB，核心引擎，代码分析，KDB 实际演练，KDB 的重要命令，准备 KGDB 调试环境（内核调试环境建立和实际演示），调试符号，使用 Ubuntu 的符号包，初始断点，kgdbwait，KGDB 中调用 KDB 命令，触发 break-in 的多种方法，/proc/kcore

第六部分：文件系统（1.5 小时）

要点：“一切皆文件”，文件系统架构，组成，文件操作，设备文件系统，使用内核调试器帮助理解文件系统，EXT FS，Reiser FS，四个核心对象，准文件系统，proc fs（原理，关键代码，重要的应用，meminfo，maps 等），sysfs，debug fs

实战 2：使用 LINUX 双机内核调试探究句柄混论之谜

应用程序与驱动程序通信时，驱动程序总是收到错误的数据，打印出来观察，竟然是日志信息送给了驱动…使用 KGDB 分析应用层程序与驱动程序间通信的过程，分析数据混乱原因，理解虚拟文件系统、Linux 驱动程序、sysfs、标准文件等理论化

第七部分：进程管理 (1.5 小时)

要点：进程和线程，LWP，任务结构体，一体二用，进程属性，线程结构体，内核态栈，寻找内核态栈的方法，调度队列，线程优先级，线程调度器，计算每个任务时间片的方法，选择当前运行任务的算法，strace，ps 命令的高级用法，pstree，top，使用 strace 做简单调优

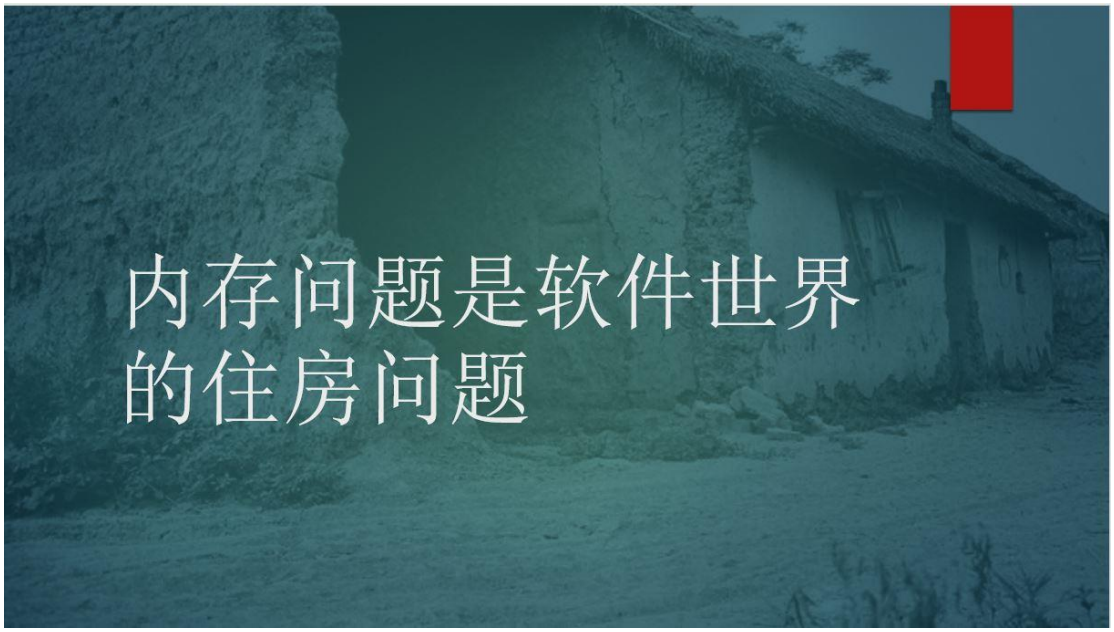
第八部分：内存管理（上）（1.5 小时）

要点：物理内存，从 core 到 DRAM，NUMA，page，pfn，页表管理，TLB，MMU，页错误，观察页错误，虚拟内存，进程的地址空间，vma，maps，vmstat，活跃内存和非活跃内

存，内核态池，从/proc/meminfo 谈内存的使，meminfo 信息深入分析

实战 3：与内存管理器对话

通过用户态和内核驱动样例程序以不同方式做分配操作，演示 meminfo 输出信息的改变，理解内存去哪儿啦以及触发 OOM killer 的过程



第九部分：内存管理（下）（1.5 小时）

要点：用户态堆，ptmalloc，arena，heap，主 arena 的布局，辅 anrena 的创建，堆块结构，分配策略，bin，bin 的组织，分配过程，释放过程，堆有关的错误，故障调试，valgrind，valgind 的工作原理

实战 4：使用 valgrind 调试典型的堆错误

堆很脆弱，经不起的考验有很多：溢出、多次释放、野指针……，在 Linux 解决这些问题的最有力武器就是 valgrind，以老雷亲自编写的 GeMalloc 程序为样本，模拟各类堆错误，并使用 valgrind 一一捕获

第十部分：内核模块和驱动程序（1.5 小时）

要点：可加载内核模块（LKM），init 和 exit，三类设备，字符设备，块设备，网络设备， softirq 和 tasklets，pnp，udevinfo，系统调用，与应用通信，ioctl, 文件读写，典型设备驱动解析 eMMC，SD，USB（控制器，HUB，设备，数据传输）

第十一部分：系统 Panic（1 小时）

要点：OOPS 和 Panic，panic_on_oops，详细解读 Oops 信息，内核转储，从 oops 消息定位代码错误，案例分享

实战 5：分析系统 Panic 的原因

随机的内核 Panic 是实际工程中常常遇到的问题，在这个动手实战中，大家将一起分析多个有代表性的 panic 案例，解析其来龙去脉，探讨分析内核 panic 的方法

```
[    30.527581] buff=.brk.early_pgt_alloc+0x0/0x6000
[    30.528101] buff=__brk_limit+0x0/0x0
[    30.529567] sym found the end c170e170
[    30.529959] end addr of symtable c170e170
[    30.530370] sym num=77734, addr=c16c22d8, name=c170e174
[    30.531141] BUG: unable to handle kernel NULL pointer dereference at 00000008
[    30.531878] IP: [<c155b660>] kallsym_init+0x140/0x260
[    30.532390] *pdpt = 0000000000000000 *pde = f000ff53f000ff53
[    30.533011] Oops: 0000 [#1] SMP
[    30.533356] Modules linked in:
[    30.533669] CPU: 0 PID: 1 Comm: swapper/0 Not tainted 3.11.0gedu #11
[    30.534311] Hardware name: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[    30.535124] task: df480000 ti: df44a000 task.ti: df44a000
[    30.535717] EIP: 0060:[<c155b660>] EFLAGS: 00010246 CPU: 0
[    30.539482] EIP is at kallsym_init+0x140/0x260
[    30.539929] EAX: 00000000 EBX: c17f6ab8 ECX: 00000009 EDX: 00000100
[    30.540559] ESI: c17f626c EDI: c17f672c EBP: df44beac ESP: df44be90
[    30.541190]  DS: 007b ES: 007b FS: 00d8 GS: 00e0 SS: 0068
[    30.541725] CR0: 8005003b CR2: 00000008 CR3: 01a62000 CR4: 000406f0
[    30.542349] DR0: 00000000 DR1: 00000000 DR2: 00000000 DR3: 00000000
[    30.542978] DR6: fffe0ff0 DR7: 00000400
[    30.543361] Stack:
[    30.543568]  c1896f18 00012fa6 c16c22d8 c170e174 00000000 00000105 c1a39cd4 df44bef8
[    30.546307]  c19ceb1e c1864976 00000060 000080d0 00000301 de3a15a0 de3a15a0 00000000
[    30.547282]  df44bee8 c13fd5bb c1b3b23c 00000000 00000105 c1a39cd0 df44bef0 c1551769
[    30.548199] Call Trace:
[    30.548454]  [<c19ceb1e>] fedcore_init+0x15/0x350
[    30.548951]  [<c13fd5bb>] ? __class_create+0x4b/0x70
[    30.549474]  [<c1551769>] ? create_extcon_class.part.2+0x19/0x30
[    30.550111]  [<c19ceb07>] ? extcon_class_init+0x13/0x15
```

第十二部分：日志和消息输出（1 小时）

要点：系统日志架构，printk，vprintk_emit，消息级别，消息头结构，结构化信息输出，facility，logger，syslog，console，syslogd，/dev/kmsg，隐含锁，动态控制消息输出，结构化的消息，结构化消息在 PnP 中的应用

第十三部分：调优基础（1 小时）

要点：性能目标示例，衡量性能的技术指标，测试性能的两种基本方法，Sampling，Instrumentation，典型的分析方法

第十四部分：事件追踪(ftrace 和 perf)（1.5 小时）

要点：trace 机制背景，ftrace 简史，ftrace 的工作原理，追踪点，文件系统接口，user marker，启用追踪，读取 trace 数据，Kernshark，使用示例，perf，选择 CPU 的计数器，perf 使用示例

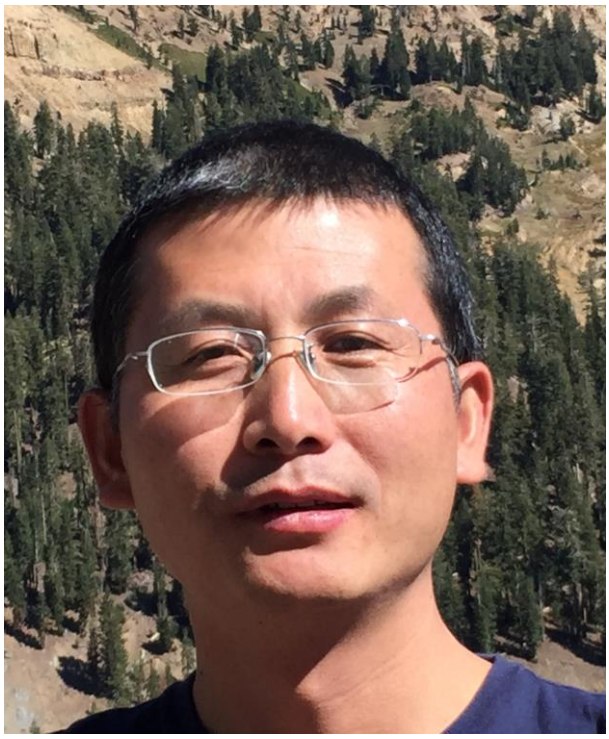
第十五部分：使用 vTune 调优（1.5 小时）

要点：vTune 背景，版本历史，工作原理，主要功能，Hotspot 分析，符号文件和符号文件设置，与 Eclipse 的集成，指定分析目标，选择分析类型，自定义分析类型，选择 CPU 的硬件计数器，视图，函数和调用栈，汇编视图，源代码视图，观察 Preemption 事件

实战 6：使用 vTune 分析 AI 应用的执行热点

通过 vTune 的监视工具采集 AI 应用的运行数据，然后使用 vTune 图形分析工具进行分析，学习不同分析视图的用法，理解 vTune 中的关键性能指标

讲师介绍



张银奎（Raymond Zhang），绰号“格蠹老雷”，1996年毕业于上海交通大学信息与控制工程系，在软件产业工作20余年，一多半时间任职于 INTEL 公司的上海研发中心，先后在PASD、DEG、CPG、PCCG、VPG等部门工作。业余时间喜欢写作和参与各类技术会议，发文数百万字，探讨各类软件问题，其中《在调试器里看阿里的软件兵团》等文章广为流传。2015年起获微软全球最有价值技术专家（MVP）奖励。著有《软件调试》和《格蠹汇编》二书，曾经主笔《程序员》杂志调试之剑专栏 。在多家跨国公司历任开发工程师、软件架构师、开发经理、项目经理等职务，对 IA-32 架构、操作系统内核、驱动程序、虚拟化技术、云计算、软件调优、尤其是软件调试有较深入研究。从2005年开始公开讲授“Windows 内核及高级调试”课程，曾在微软的 Webcast 和各种技术会议上做过《Windows Vista 内核演进》、《调试之剑》（全球软件战役研究峰会）、《感受和思考调试器的威力》（CSDN SD2.0 大会）、《Windows 启动过程》、《如何诊断和调试蓝屏错误》、《Windows 体系结构——从操作系统的角度》（以上三个讲座都是微软“深入研究 Windows 内部原理系列”的一部分）等。翻译（合译）作品有《现代 x86 汇编语言编程》、《21 世纪机器人》、《观止——微软创建 NT 和未来的夺命狂奔》、《数据挖掘原理》、《机器学习》、《人工智能：复杂问题求解的结构和策略》等。

程煜明，1998 年毕业于上海交通大学惯性导航专业，获得博士学位，毕业后从事很多年嵌入式系统软件开发，早期的五年在上海贝尔专注电信设备上实时操作系统 PSOS/vxWorks 的底层软件开发，业余时间用调试器分析过 pSOS/vxWorks 内核的实现，后来又用了十年时间在 RadiSys 和英特尔亚太研发中心从事 Linux 底层软件的开发，曾先后在英特尔的 IMG、VPG 等部门工作，对 bootloader、Fibre channel driver、英特尔显卡驱动（I915 display driver）、40GB Ethernet user mode driver、Linux build 系统以及板级的信号完整性有深入的研究，目前对算法设计与分析比较感兴趣。

附录 1：往届研习班部分照片

附录 2：报名与收费

标准收费：**5600 元每人**

包括：

- 包含研习材料的 U 盘一个
- 研习班讲义的电子版本和纸质版本
- 研习班期间的午餐和茶点

优惠条款：

1）同一单位 6 人同时报名，可免其中一人费用

2）8 月 31 日前报名可以享受 8 折优惠

报名或垂询

1）联系课程顾问：

a) Lisa Zhang ，微信：13801874134，电子邮件：lisa.zhang@leshanting.cn

b) Cindy Long，电话：13621638537，电子邮件：809825433@qq.com

2）扫描文末的二维码，关注“格友”公众号后，直接发送报名信息或者提问。

公司付款

收款单位：上海曜印网络科技有限公司

银行账号：1001122409003035262

开户行：中国工商银行上海分行静安新城支行