Win内核的今天与未来

Windows Kernel's today and future

自我介绍

- 陈炫
  - 技术总监
  - 目前就职于北京某企业 研发中心
  - 曾参与杭州SECON云安全项目核心防护设计与实现、多个国内外渗透测试项目
  - 最近专注于p2p构建、智能技术...

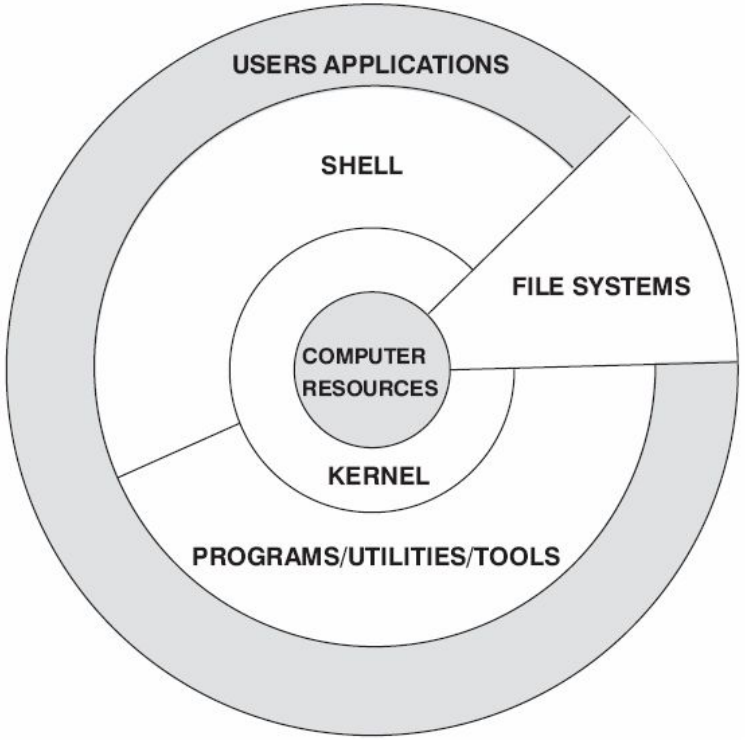
要点

1. 介绍
2. 应用领域
3. 内核安全
4. 现状及发展

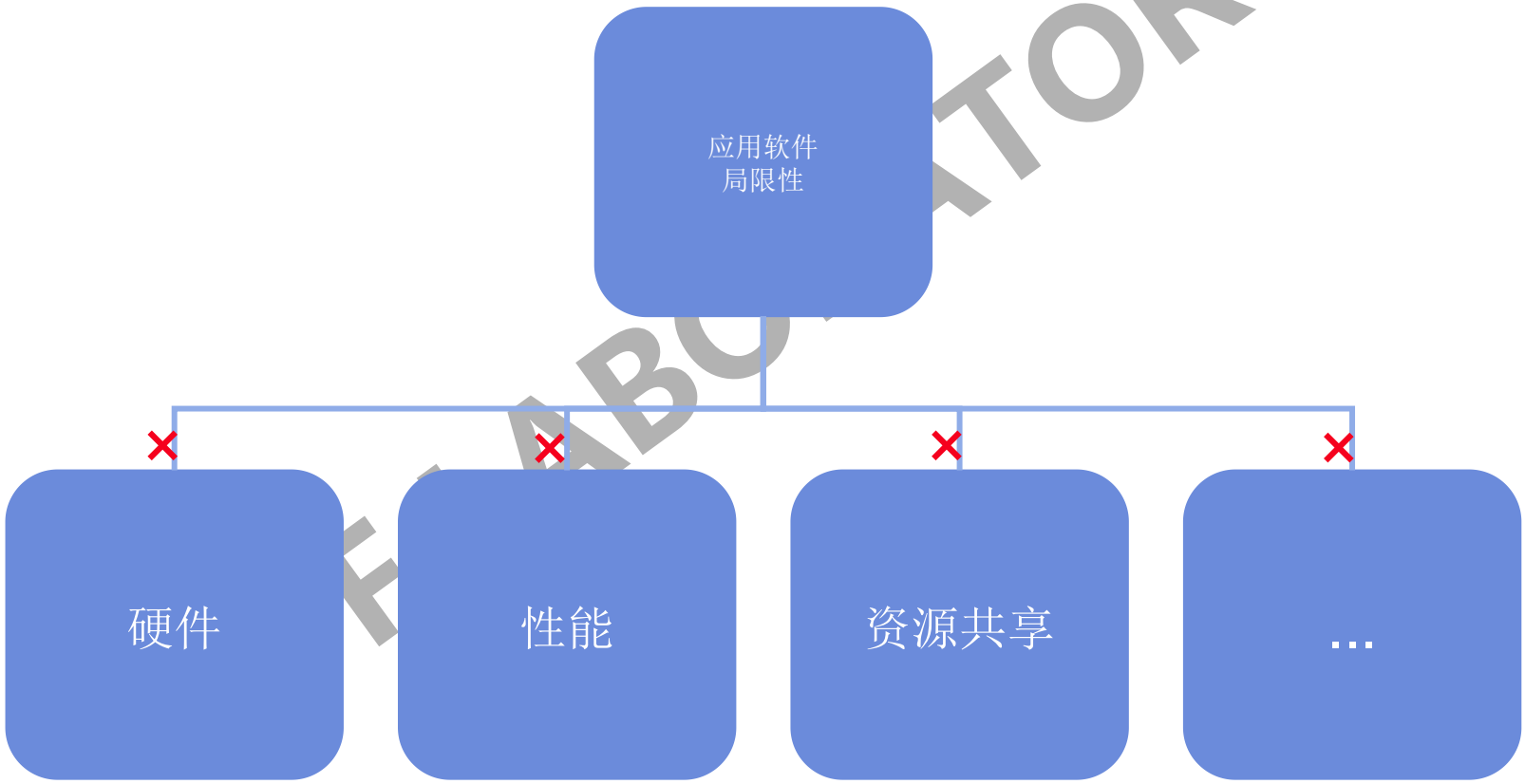
什么是内核？

- 基本介绍

- 内核分类
  - 单内核
  - 微内核
  - 混合内核



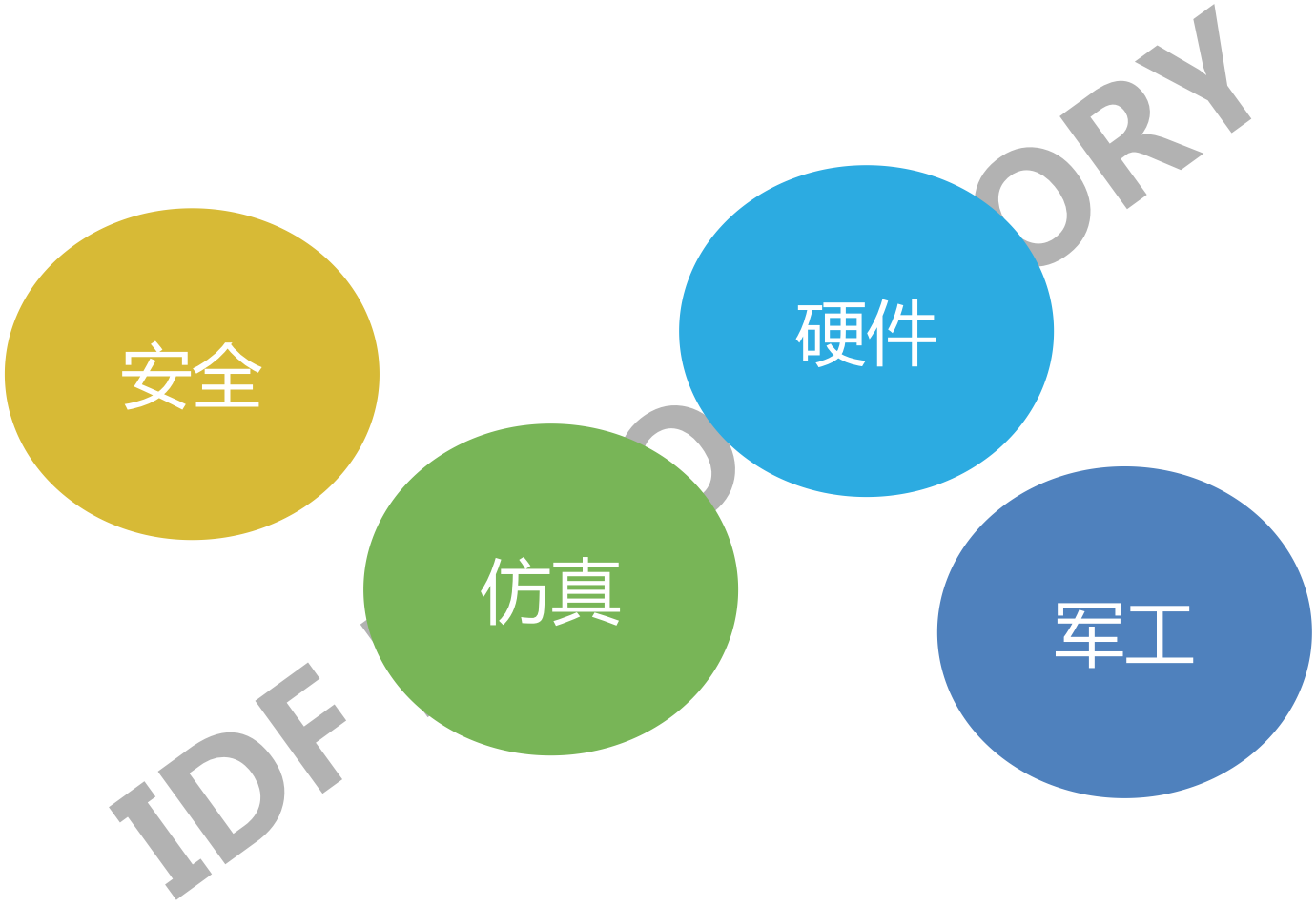
为什么需要内核开发?



在内核中我们能做什么？

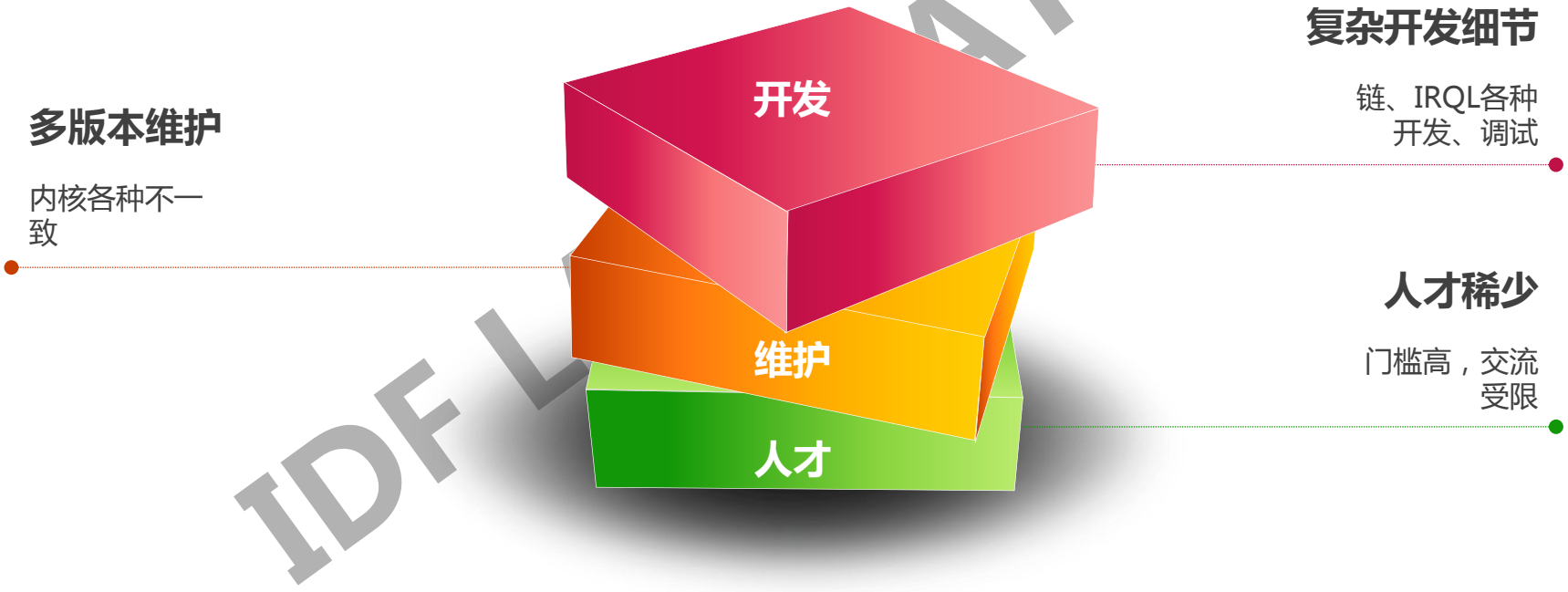
- 直接硬件级通讯及实现
- 系统级操作实现
- 探索内核底层实现细节...

应用领域



内核安全

现状



多版本维护

内核各种不一致

复杂开发细节

链、IRQL各种开发、调试

人才稀少

门槛高，交流受限

原始的字符串处理

① 申明局部变量

② 申请内存空间

③ 设置内存空间

④ 拷贝字符串

⑤ 使用...

⑥ 释放字符串

(如果局部变量为申请的内存空间，则还需释放变量自身的空间)

```
VOID TestCmpSting()

{

    UNICODE_STRING string1;
    UNICODE_STRING string2;

    RtlInitUnicodeString(&string1, L"tet");
    string2.Buffer = (PWSTR)ExAllocatePool(PagedPool, BUFFER_SIZE);
    string2.MaximumLength = BUFFER_SIZE;

    RtlCopyUnicodeString(&string2, &string1);

    if (RtlCompareUnicodeString(&string1, &string2, TRUE) == 0)
    {
        KdPrint(("1.相等\n"));
    }

    if (RtlEqualUnicodeString(&string1, &string2, TRUE))
    {
        KdPrint(("相等！\n"));
    }
    else
    {
        KdPrint(("不相等\n"));
    }
}
```

我们正在做的一些工作...

- 建立基于内核编码的开源库...
  - 简化开发流程
  - 平台兼容性

- 建立内核开放式交流社区

改进后的字符串处理

1. 使用简化
2. 隐藏复杂的实现细节
3. 检查问题更容易
4. 让更多的思维与精力在逻辑结构上...

```
BOOLEAN
    CFileName::GetParentPath(
    __in    CKrnlStr* Path,
    __inout CKrnlStr* ParentPath
    )
{
    BOOLEAN     bRet    = FALSE;
    PWCHAR      Postion = NULL;
    ULONG       Count   = 0;
    CKrnlStr    Str;


    __try
    {
        if(!Path->Get() || !ParentPath->Get())
            __leave;

        if(!ParentPath->Set(Path))
            __leave;
```

发展

1. 简易入门性
2. 培训机构或大学专业课的开设
3. 开放式的技术交流活动
4. 越来越多的讨论社区，圈子
5. 开源?

完！

谢谢

关注IDF实验室

黑客沙龙QQ群：204267310

腾讯微博：@NeteasyIDF　　新浪微博：@IDF实验室

公共微信：@IDF实验室

IRC频道：#idf_lab　　IRC服务器：irc.freenode.net