



补丁二进制比较技术

Hume

Ø 补丁比较 - 揭示差异信息的常用方法

è 补丁比较的需求

è 开源软件 Vs. 闭源软件

è 二进制补丁比较的难点

Ø 二进制文件比较的常用方法及缺陷

è 二进制字节对应比较

è 反汇编 -> 文本比较

è 其他方法

è 基于指令相似性的图形化比较(razor)

è 结构化比较(halvar flake)

è 这些方法的一些问题

Ø 理解程序本质以及补丁比较的特殊性

17. è 函数 -> 指令

è 补丁比较的特殊性

Ø 进行补丁比较

è 结构化比较、语意敏感分析



X'con 2004

è 设计签名

è 筛选(WI)

è 图的生成及查看

Ø 补丁分析实例

è Microsoft Windows schannel.dll PCT1 协议

实现远程缓冲区溢出漏洞

√ 补丁比较的需求

- × 安全防护：漏洞分析、病毒变种分析
- × 利用其他产品未公开特性的产品
- × 别有用心的黑客

√ 开源软件 Vs. 闭源软件

- × 开源软件补丁 > 源代码对比比较简单

X'con 2004

X 闭源软件补丁 >< 二进制比较

V 二进制补丁比较的难点

X 一个补丁补多个问题，代码变化较多

X 与补丁无关的其他变化

X 编译器优化

è 源码修改编译 <-> 逆向工程，信息不对称

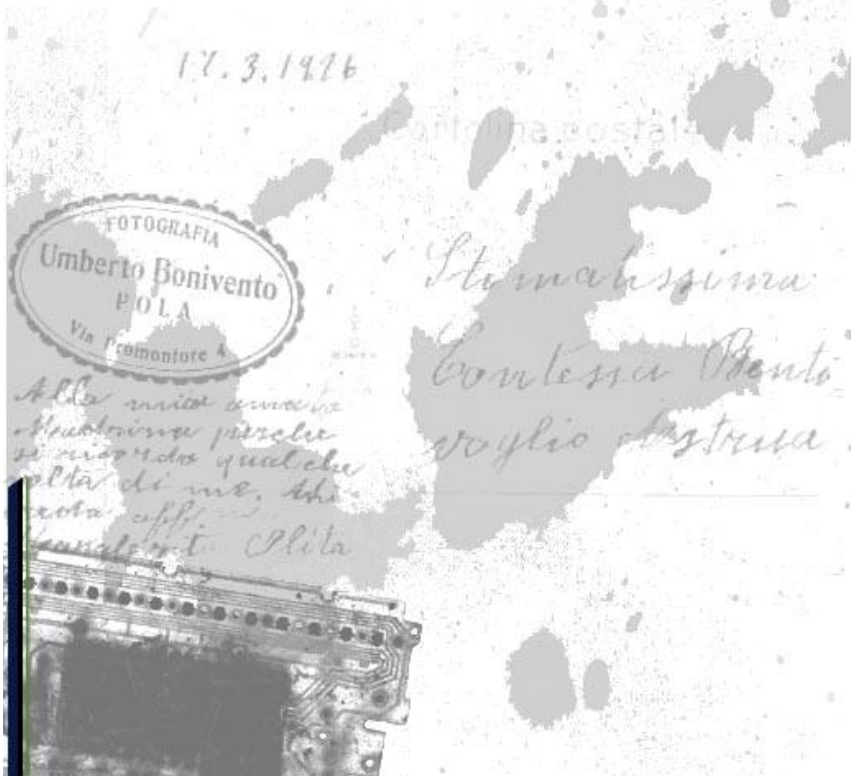
è 传统比较方法已经不能适应补丁比较的最新需要

- √ 二进制字节对应比较。FC，只适用于极少量的变化（若干字节）的补丁比较
- √ 反汇编 -> 文本比较。Beyond compare, vi, emacs... 缺乏对程序逻辑的理解，只适用于小文件和少量变化
- √ 其他方法。正则表达式结合文本比较？

√ 基于指令相似性的图形化比较。

Todd Sabin: 《Comparing binaries with graph isomorphisms》

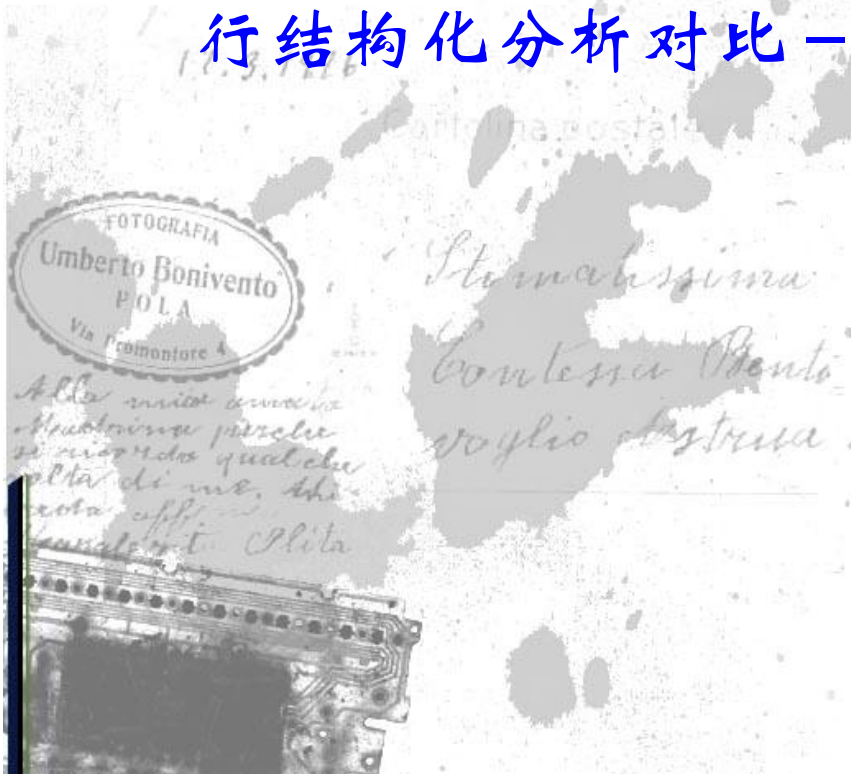
Ⓟ 函数对比 - 每条指令作为流程图的一个节点 -
流程图化简 - 流程图合成 - 人工分检对比



√ 结构化比较

Halvar Flake: 《Structural Comparison of Executable Objects》

▷ 结构化函数签名 (逻辑块数, 子调用数目, 链接数)
配比 - 签名相同不能匹配函数通过函数调用树进行结构化分析对比 - 得到结果



√ 两种方法各自的优点

⊞ 结构化签名与具体平台无关，便于移植

⊞ 结构化签名不会受到部分编译器优化的影响

⊞ 指令相似性的图形化比较不会漏掉非结构化变动（尽管这种情况不多）

⊞ 图形化比较相当直观



√ 两种方法各自的问题

→ 结构化签名对比不能找出非结构化变动

→ 结构化签名相同的函数较多,完全用结构化签名+结构化配比后仍可能导致部分函数无法匹配

→ 上层函数结构化配比错误后的瀑布效应

→ 指令相似性对比受编译器优化困扰

→ 相似图形的化简存在不完全的问题

✓ 有序指令序列

指令：操作码[动作] 操作数[动作对象]

✓ 函数作为基本逻辑单元

✓ 软件工程：接口(其实现)作为基本的功能单元

✓ 增量链接

- √ 两个二进制文件非常相似，差异函数一般低于全部的20%
- √ 经常由同一编译器或同系列编译器编译
- √ 大部分二进制代码不变
- √ 部分被修改模块的编译器优化

è 目的：找出被修改函数的语意变化

√ 屏蔽底层差异 -> 反汇编为统一的高级语言或中间语言

à 编译器千差万别，尚无成熟技术

√ 有向图对比

à 图形相似对比 - NP问题

Ú 现实：速度及计算能力 - 理想情况的近似解决，
可产生可用的结果

ü 结构化比较

è 整个文件视为“图”

è 函数作为基本逻辑单位 — “子图”

è 找到比较起始点

è 开始比较

è 不同函数的结构化配比，标识不同函数之间的
对应关系

ü 设计函数签名

è 平台无关签名

† 逻辑块数 - 子调用数 - 逻辑链接数

† 逻辑块数 - 子调用数 - 逻辑链接数 - 指令数

† 逻辑块数 - 子调用数 - 逻辑链接数 - 其他平台无关特征

È 设计你自己的签名

Ð 平台无关签名便于移植，简单规则可对付分支优化

à 部分结签名是不精确的，要结合结构化分析来确定精确匹 配点

ü 设计函数签名(续)

è 平台相关签名

† IDA Flirt签名

† 指令顺序相关(不敏感)的签名

† 指令顺序无关签名

17.3.19† (指令-操作数)类型签名

È 消除重定位的影响, 设计你自己的签名

ü 设计函数签名(续)

▮ 可进行精确匹配,适当设计的签名可对付
寄存器置换等变动

▮ 增加匹配函数数目,减少平台无关签名错误带来的
后续瀑布效应

à 不便于移植,较难对付分支优化

ü 结果筛选(WI – weak intelligence)

à 每种签名都有其弱点和不足

à 各种签名结果之间的差异可揭示某些问题的所在

è 综合各种签名,不应漏掉差异

è 最终结果的分析判定只能靠人工进行

è 通常在人工干预下进行结果筛选(取各种签名对比结果的交集或差异集或并集,消除库函数以及其他已知无效函数的影响)可减轻比较分析的难度以及劳动量

ü 图形化比较 - 图的生成及查看

▷ 函数流程图的生成是比较简单的(vcg)

▷ 图形显示比较困难,但存在现成工具和库

17.3.197 Win32graph

AiSee

▷ 人对图形差异优于对文本差异的直观感知

è 流程图的生成及差异染色

Microsoft Windows schannel.dll PCT1 协议实现远程缓冲区溢出漏洞

程序对比补丁前后schannel.DLL后大约产生20个左右的差异函数,进一步人工分析注意到_Pct1SrvHandleUniHello补丁前后发生了变化:

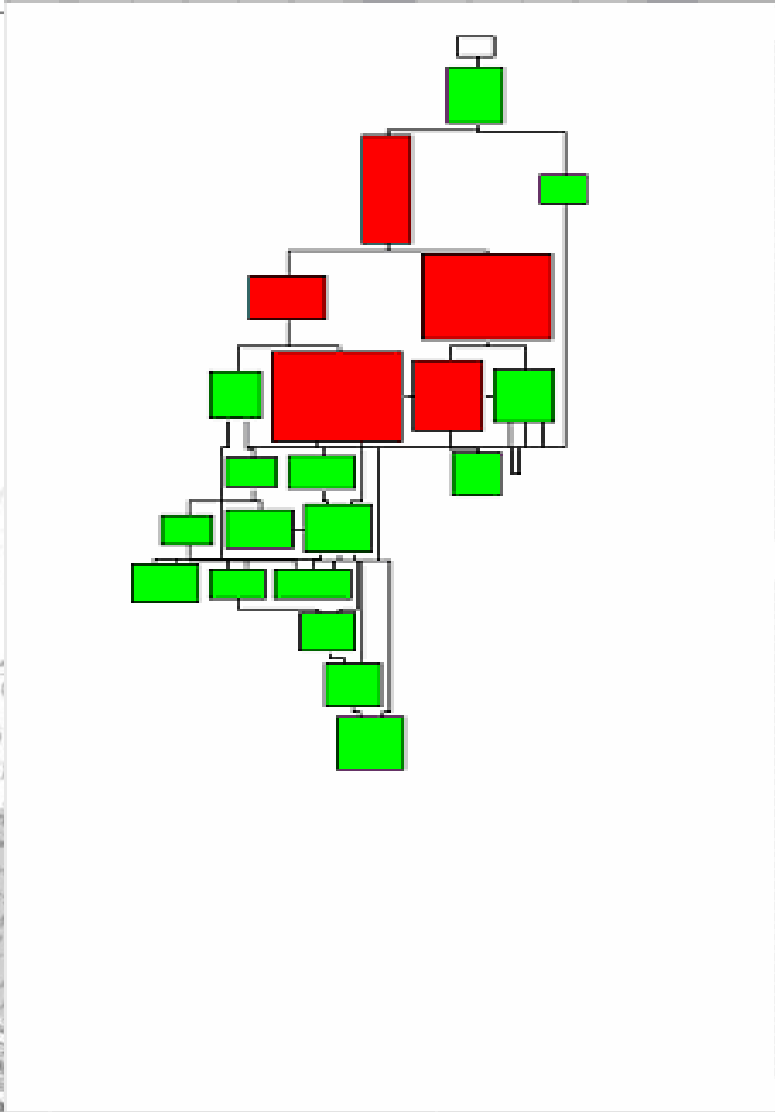
```
.text:766AE2BD      mov     [ebp+8], eax
.text:766AE2C0      mov     eax, [edx+0Ch]
.text:766AE2C3      lea    ebx, [eax+eax]
.text:766AE2C6      cmp    ebx, 20h
.text:766AE2C9      jbe    short loc_766AE2D2
```

进一步分析可知该漏洞为栈溢出



WinGraph32 - Graph Visualization b...

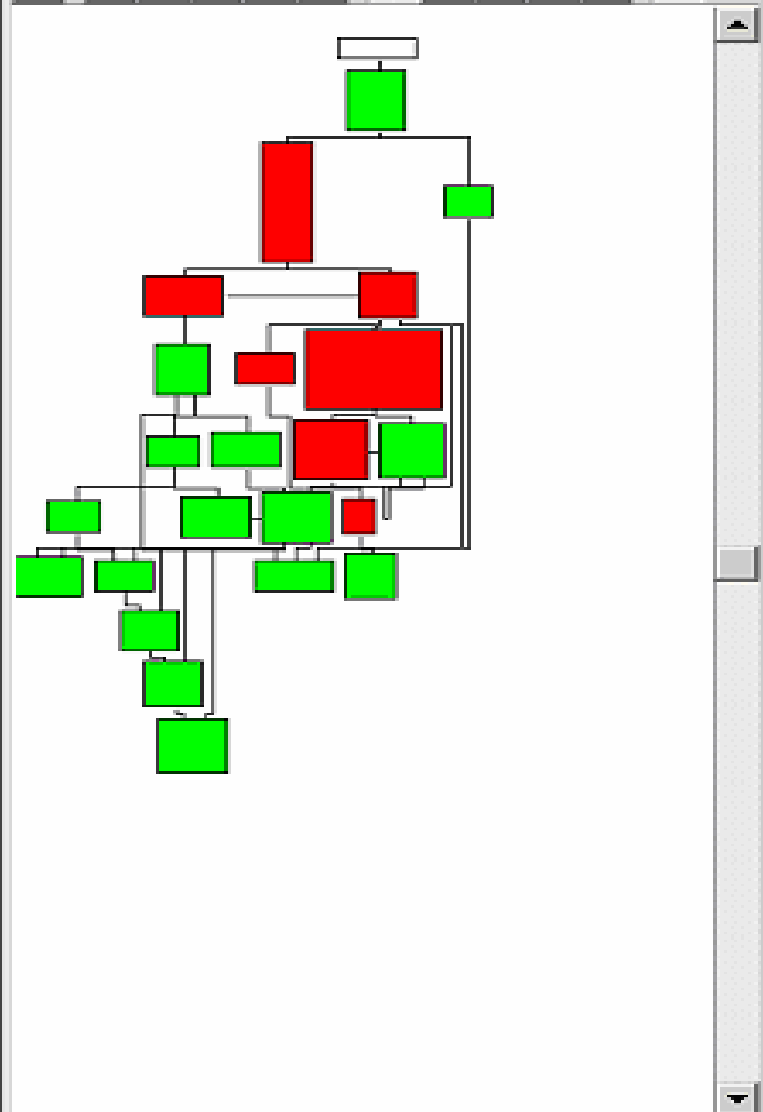
File View Zoom Move Help



16.26% (52,16) 22 nodes, 47 edge segments, 10

wii 拼自加加 Graph Visualizati...

File View Zoom Move Help



17.09% (-2.15) 24 nodes, 53 edge segments

FOTO
Umberto
P/O
Via Icom
Alle r
Murotri
si ricor
alta d
rota c
laurale

√ MS04-11 LSASRV.DLL补丁前后对比

Ú 对比后差异函数不到20个,部分输出如下:

?NegpCrackRequest - sub_742DBEB0

?NegpDetermineTokenPackage - sub_742FB2E0

?SetFlags - sub_74319CF0

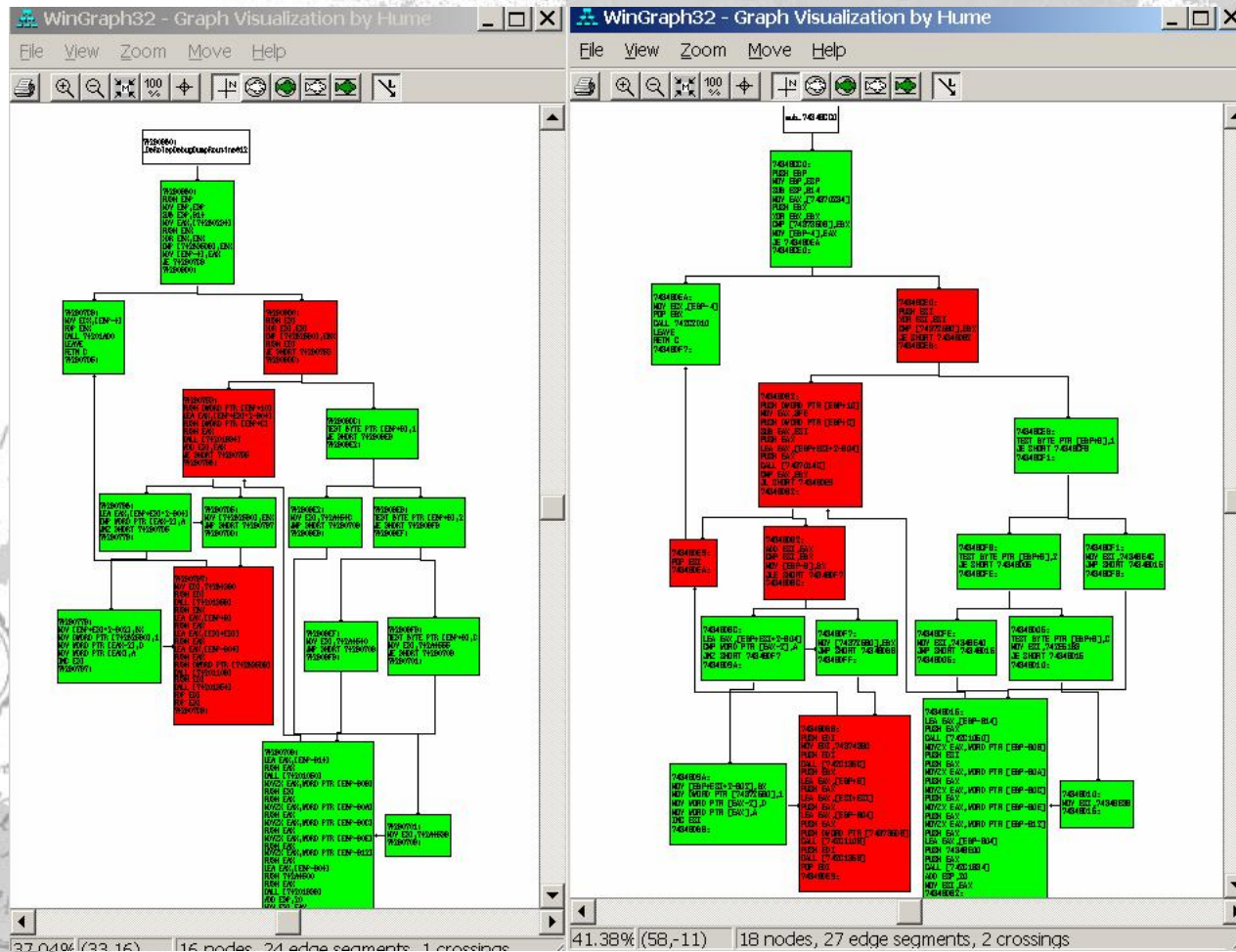
_LsapDbOpenTrustedDomainByName - sub_74321A80

_DsRolepDebugDumpRoutine - sub_74346CC0

Ú 经过分析其中两个函数分别修补了两个漏洞:

其中一个就是后来被振荡波等病毒利用的

DsRolepDebugDumpRoutine远程栈溢出漏洞



```
74280753:  
PUSH DWORD PTR [EBP+10]  
LEA EAX,[EBP+ESI*2-804]  
PUSH DWORD PTR [EBP+C]  
PUSH EAX  
CALL [74201634]  
ADD ESI,EAX  
JE SHORT 742807D5  
7428076B:
```

```
74346D62:  
PUSH DWORD PTR [EBP+10]  
MOV EAX,3FE  
PUSH DWORD PTR [EBP+C]  
SUB EAX,ESI  
PUSH EAX  
LEA EAX,[EBP+ESI*2-804]  
PUSH EAX  
CALL [7437014C]  
CMP EAX,EBX  
JL SHORT 74346DE9  
74346D82:
```

```

add     esp, 20h
mov     esi, eax
; CODE XREF: D
push   [ebp+arg_8]
lea    eax, [ebp+esi*2+var_804]
push   [ebp+arg_4]
push   eax
call   ds:__imp__wvsprintfW@12 ; __de
add    esi, eax
jz     short loc_742807D5
lea    eax, [ebp+esi*2+var_804]
push   [ebp+psz1] ; CODE >
mov    eax, 3FEh ; 参数1
push   [ebp+pszfmt] ; pszfmt
sub    eax, esi
push   eax ; cchLin
lea    eax, [ebp+esi*2+Buffer]
push   eax ; lpout
call   wvsprintfW
cmp    eax, ebx ; EAX==I
jl     short loc_74346DE9
add    esi, eax

```

谢谢！
Thanks！

POST CARD

DATE

Comandante



STUDIO FOTOGRAFICO
DANTE MORONI
Via S. ... N. 16
TORINO

17.3.1926

Ufficio postale

FOTOGRAFIA
Umberto Bonivento
PIOLA
Via Comandante 4

Stimabilissima
Contessa Monto
voglio ringraziarla

Alle uniche amiche
che mi sono rimaste
si ricordi qualche
volta di me. Mi
resta aff.
Umberto Piola



Any Questions?

