Canape – Bytes your Bits

James Forshaw and Michael Jordon

context
INFORMATION SECURITY LTD

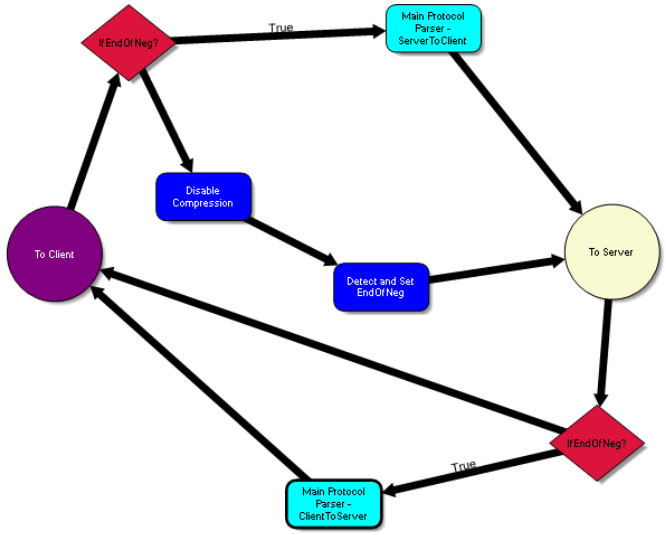
What we are going to talk about?

- New tool released at Blackhat – Canape
- What is Citrix ICA?
- In Canape:
  - MitM ICA
  - Fuzz ICA
  - Exploit ICA
- 0 Day

context
INFORMATION SECURITY

What is Canape?

- Binary Network Application Testing Tool
- Existing tools:
  - HTTP proxies (e.g. CAT)
  - Echo Mirage
  - Python libraries
  - Custom code
  - Wireshark
- Why a new tool?
  - Has these features and more
  - All driven through a GUI
- And it's free!



context
INFORMATION SECURITY

How does it MitM?

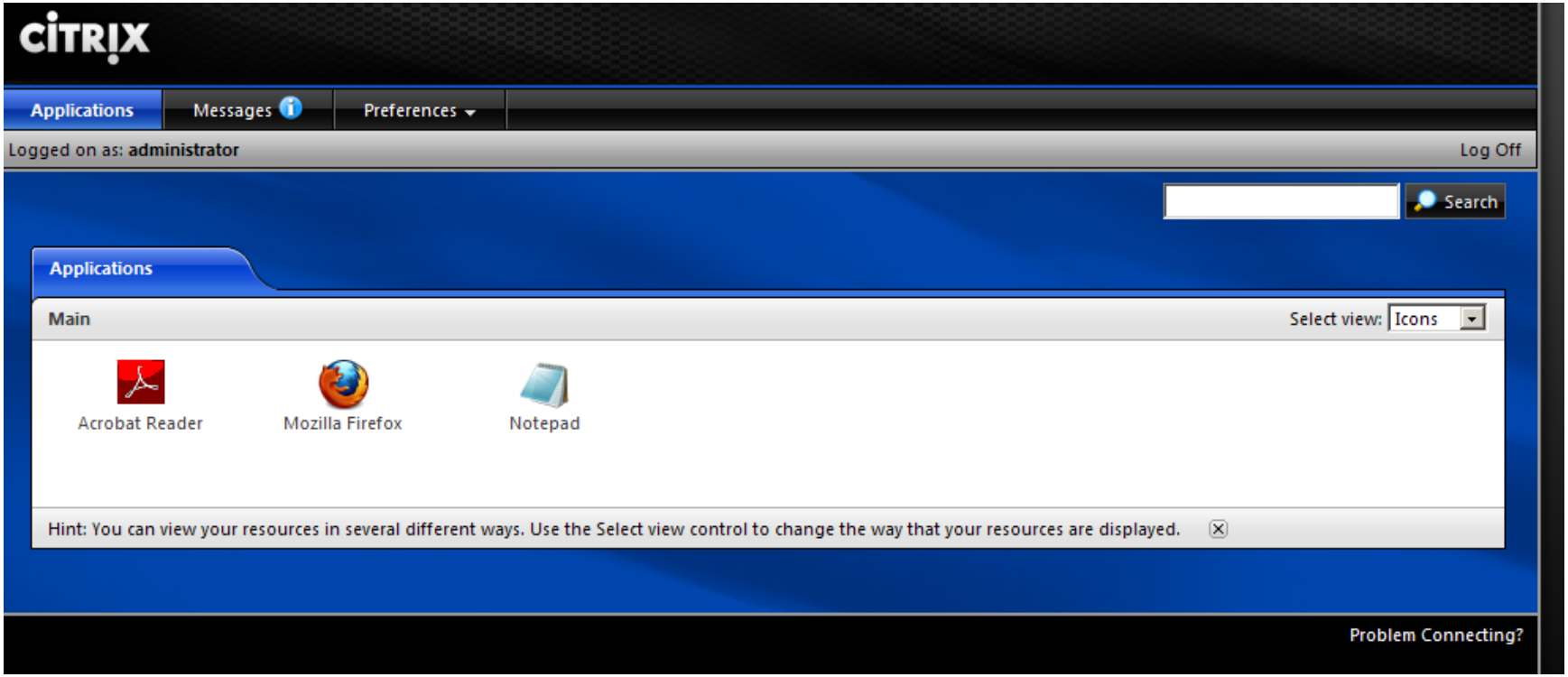
- MitM support:
  - SOCKS
  - Port forwarding
  - TCP, UDP, HTTP, Broadcast
  - SSL
- Pipelines

context
INFORMATION SECURITY

What is ICA?

- Protocol used for Citrix XenApp and XenDesktop products
- Remote desktop and applications
- Uses a bespoke client
- Needs a suitable configuration file to connect

Citrix Web Interface



context
INFORMATION SECURITY

The ICA File

```
[WFClient]
Version=2
TcpBrowserAddress=10.0.131.190
ICASOCKSProtocolVersion=0
ICASOCKSProxyHost=127.0.0.1
ICASOCKSProxyPortNumber=1080

[ApplicationServers]
10.0.131.190=

[10.0.131.190]
Address=10.0.131.190
InitialProgram=
```

context INFORMATION SECURITY

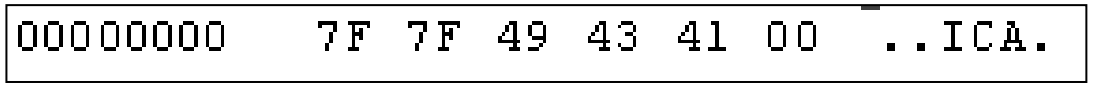
Demo 1

- MitM ICA traffic

context
INFORMATION SECURITY

ICA Protocol

- Stream based protocol
- Single TCP stream
- Phases
  - Hello
  - Negotiation
  - Main stream
    - Encrypted
    - Compressed
    - Multiplexed



Demo 2

- Handling state transitions

ICA Main Protocol

- Main protocol is wrapped in a simple frame
- 12 bit byte length
- 4 bit flags

context
INFORMATION SECURITY

Demo 3

- Parsing the framing

Basic ‘Encryption’

Data	Length	Hash
▯ICA\x00	6	3FF3B3...
\x01¢\x00¢\x00"\x00\x01\x08WFICA32.EXE\x00\x00\x00\x0...	3082	5B07D7...
\x04\x00\x00	3	740EA5...
\x03\x00\x04\x00\x1C	5	0C6A70...
\x1B\x00\x01c;37+7+7+7+7+7+';6"6"\x18ú	29	69565F...
\x05\x00\x01æóí\x0F	7	1617A4...
°E\x01;\x14\x08▯àôúä▯▯▯▯▯▯▯▯▯ù¾\x14Õ▯\x17▯\x1FT¼Ó4▯Æ▯Ò$%...	2171	DE0D6...
[illegible]	76	[illegible]

Data	Length	Hash
▯ICA\x00	6	3FF3B3...
\x01¢\x00¢\x00"\x00\x01\x08WFICA32.EXE\x00\x00\x00\x0...	3082	AF730D...
\x04\x00\x00	3	740EA5...
\x03\x00\x04\x00d	5	CCB4C7...
\x1B\x00\x01#\x03s\x17w\x13w\x13w\x13w\x13w\x13w\x13...	29	B1ABEE...
\x05\x00\x01¦E-7	7	6D3B28...
°E\x01{\x11u▯ñ▯áà▯é▯é▯è▯é▯Ç¥S\x1FPf\x00!\x11\x1D·▯N▯▯Rj0,r...	2171	3B3A52...
L@\x01,C'Ã▯÷▯·Ó¶Ò¤ÀÛÍI?"\x18ëð°E&¬(ë&\x01ë\x01d\x00p\x...	78	67B4D8...

context
INFORMATION SECURITY

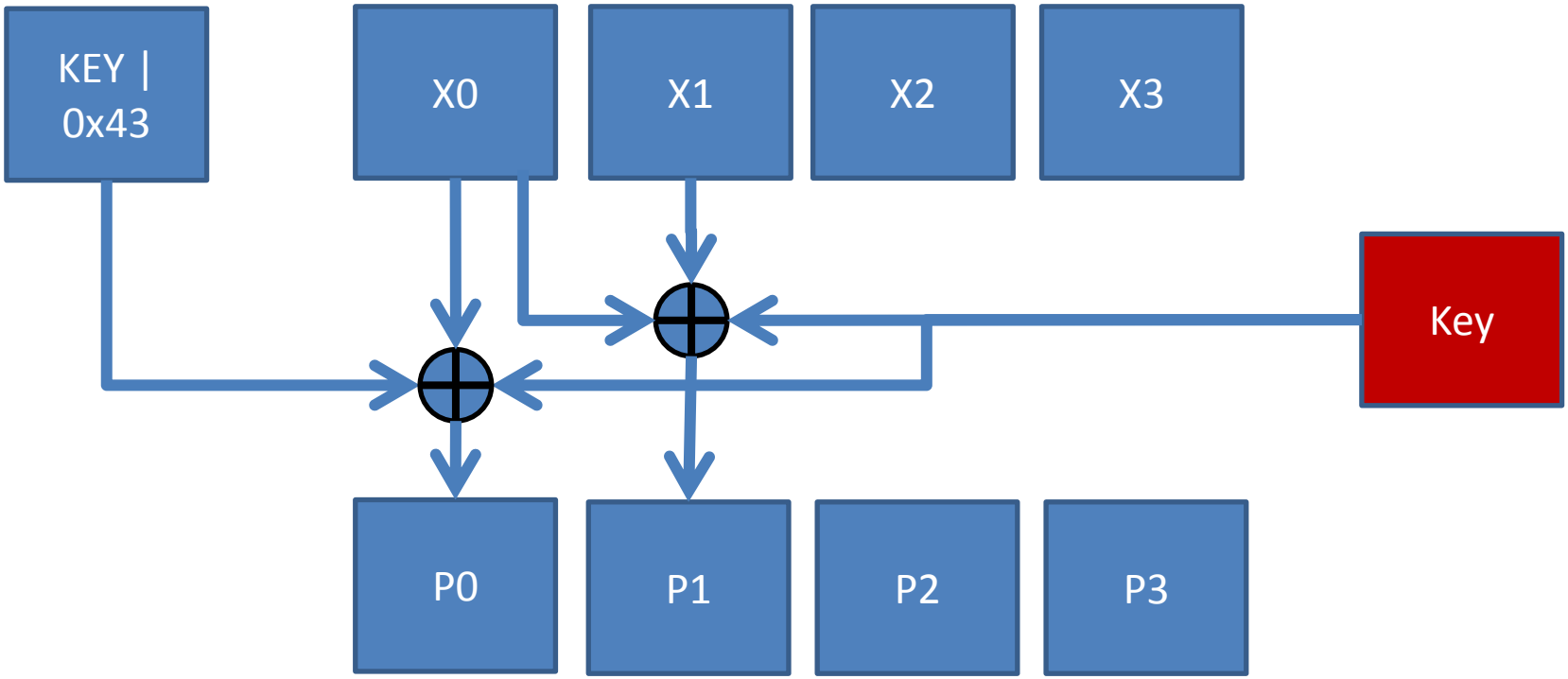
The 'Encryption'

```
public EncryptProtocolDriver()
{
    super(false, g);
    h = false;
    i = false;
    l = (byte)(new Random()).nextInt();
    j = (byte)(l | 0x43);
    k = (byte)(l | 0x43);
}

private final void b(byte abyte0[], int i1, int j1)
{
    int k1 = (i1 + j1) - 1;
    byte byte0 = abyte0[k1];
    byte byte1 = l;
    for(int l1 = k1; l1 > i1; l1--)
        abyte0[l1] ^= abyte0[l1 - 1] ^ byte1;

    abyte0[i1] ^= j ^ byte1;
    j = byte0;
}
```

Encryption Diagram



Demo 4

- MitM the encrypted XOR stream

Compression

- Registry key
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP\Compress = Off`

```
00000180   57 44 49 43 41 00 00 00 00 0B 3F 49 5C A8 C1 26   WDICA.....?I\¨Á&
00000190   00 BF 60 29 4B 1C 02 DC 07 0D 03 2E 3C 0F 00 00   .¿`)K..Ü....<...
000001A0   00 00 00 00 00 88 13 2C 00 2C 00 FF FF FF FF 01   .......,.,.ÿÿÿÿ.
000001B0   00 00 00 00 00 1A 00 56 00 10 12 00 00 03 00 4F   .......V.......O
000001C0   01 5A 01 43 54 58 54 57 20 20 00 09 00 43 54 58   .Z.CTXTW  ...CTX
```

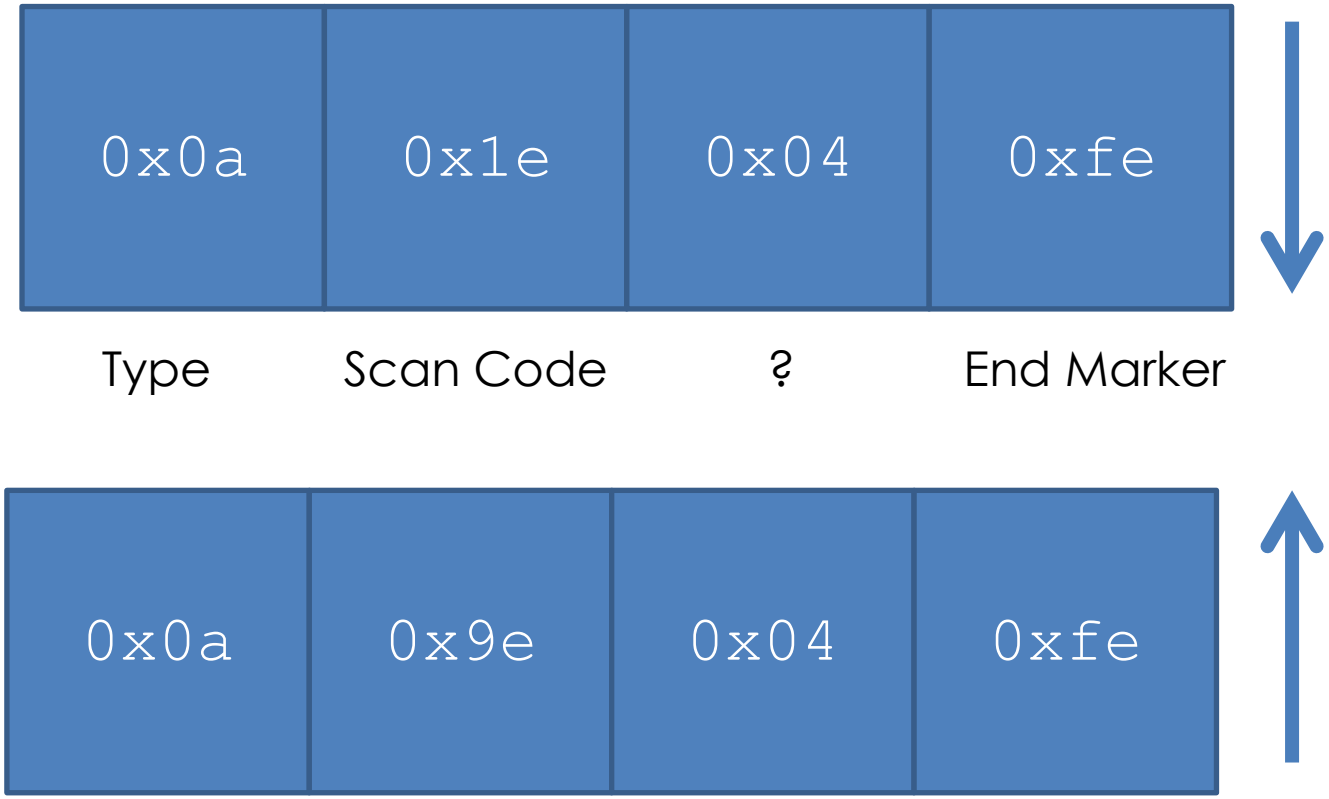
```
00000180   57 44 49 43 41 00 00 00 00 0B 3F 49 5C A8 C1 26   WDICA.....?I\¨Á&
00000190   00 BF 60 29 4B 1C 02 DC 07 0D 16 20 01 0F 00 00   .¿`)K..Ü... ....
000001A0   00 00 00 00 00 88 13 2C 00 2C 00 FF FF FF FF 01   .......,.,.ÿÿÿÿ.
000001B0   00 00 00 00 00 1A 00 56 00 00 00 00 00 00 00 4F   .......V.......O
000001C0   01 5A 01 43 54 58 54 57 20 20 00 09 00 43 54 58   .Z.CTXTW  ...CTX
```

context
INFORMATION SECURITY

Demo 5

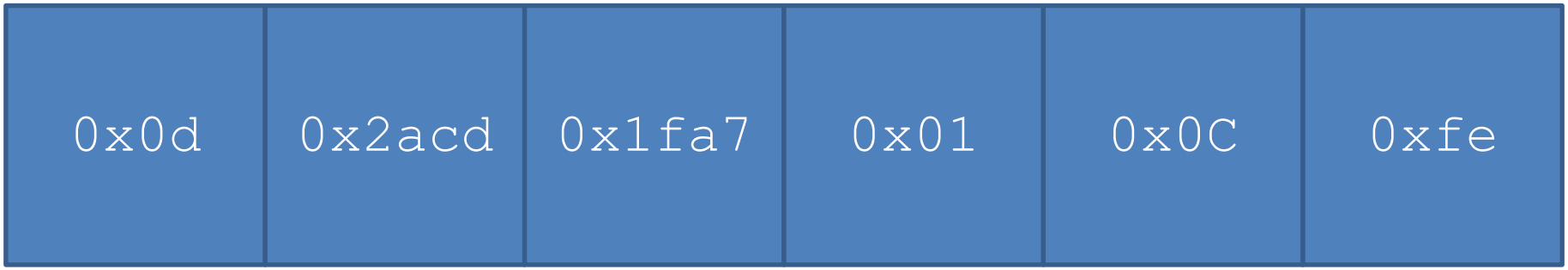
- Downgrade to no compression
- Replace:
  - 0x00 0x10 0x12 => 0x00 0x00 0x00

Key Press



context
INFORMATION SECURITY

Mouse Movement



Button State

01 – No Buttons
02 – Press Left
04 – Release left
08 – Press Right
10 – Release Right

context INFORMATION SECURITY

Fuzzing

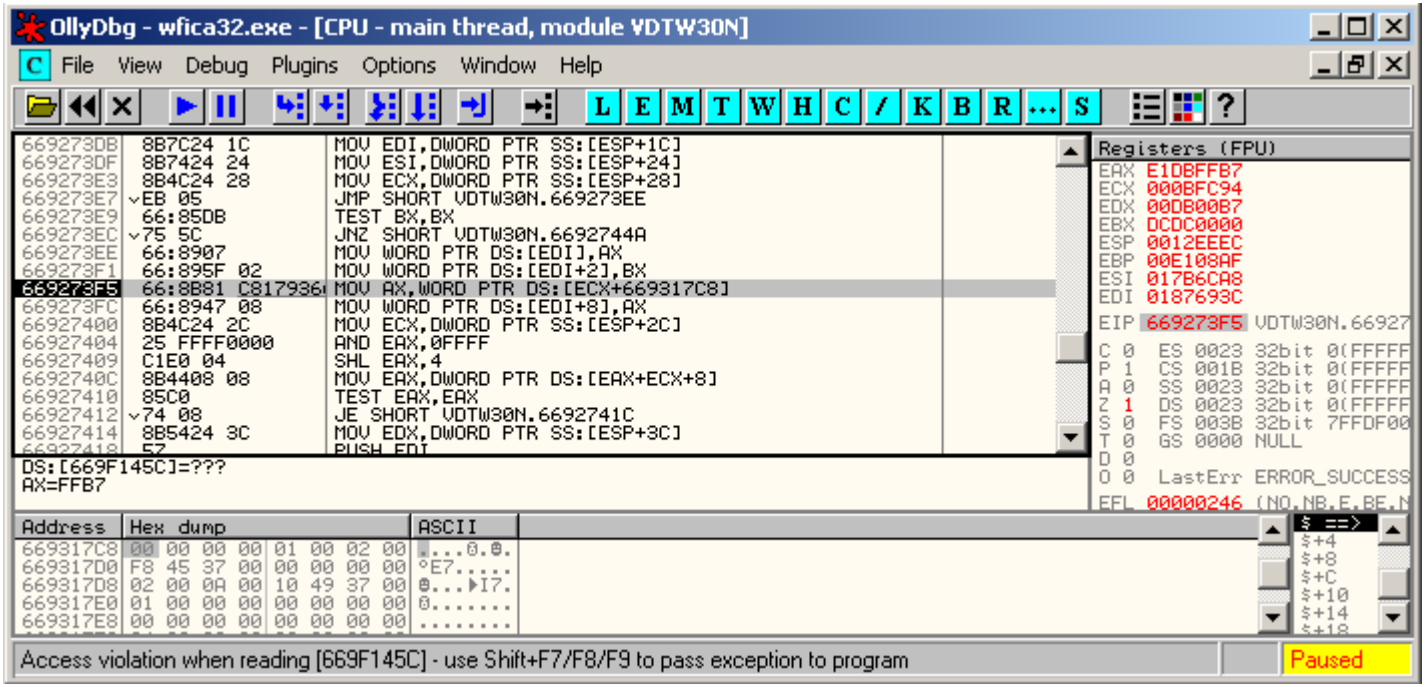
- Standard fuzzing
  - But we are in the encrypted and compressed stream
- Byte fuzzing

context
INFORMATION SECURITY

Demo 6

- Fuzz the contents of the encrypted stream

context
INFORMATION SECURITY



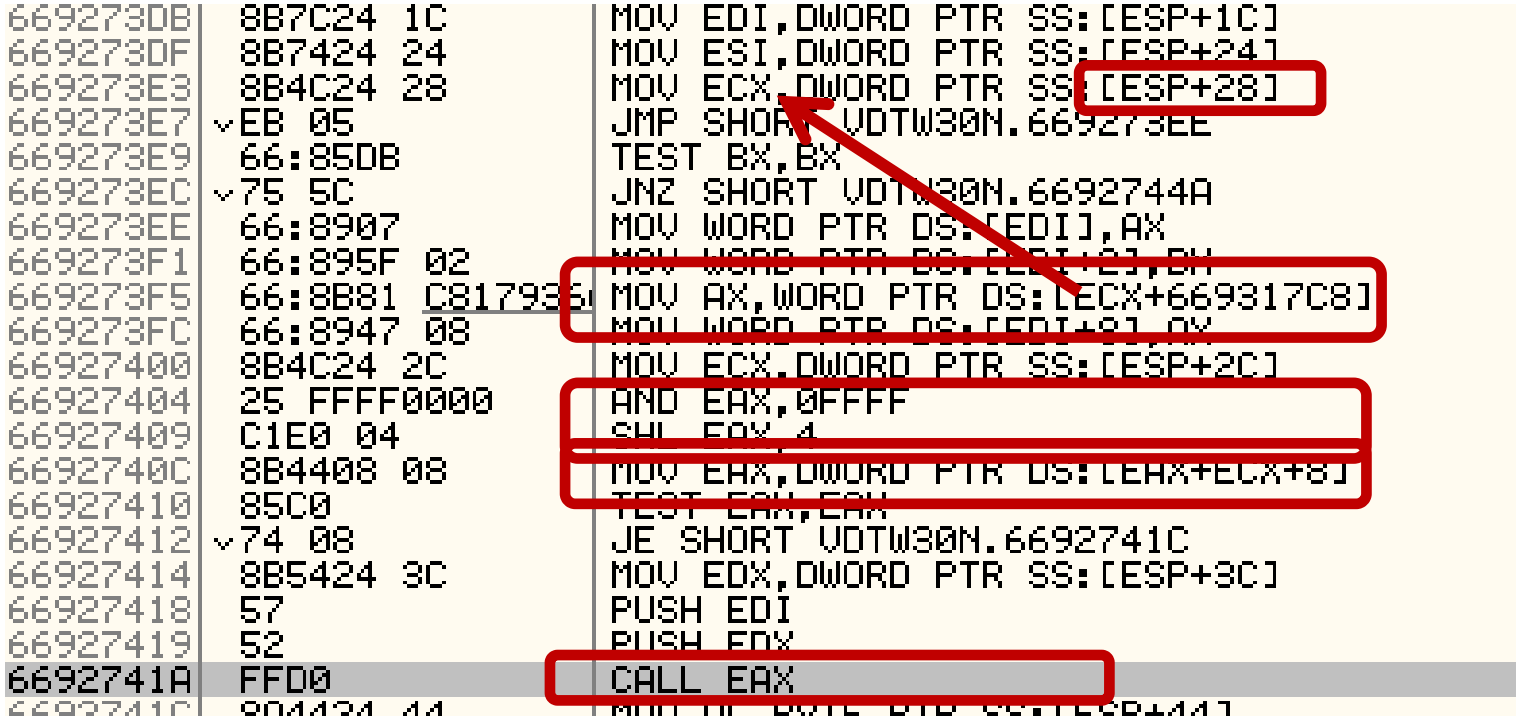
Access violation when reading [669F145C] -

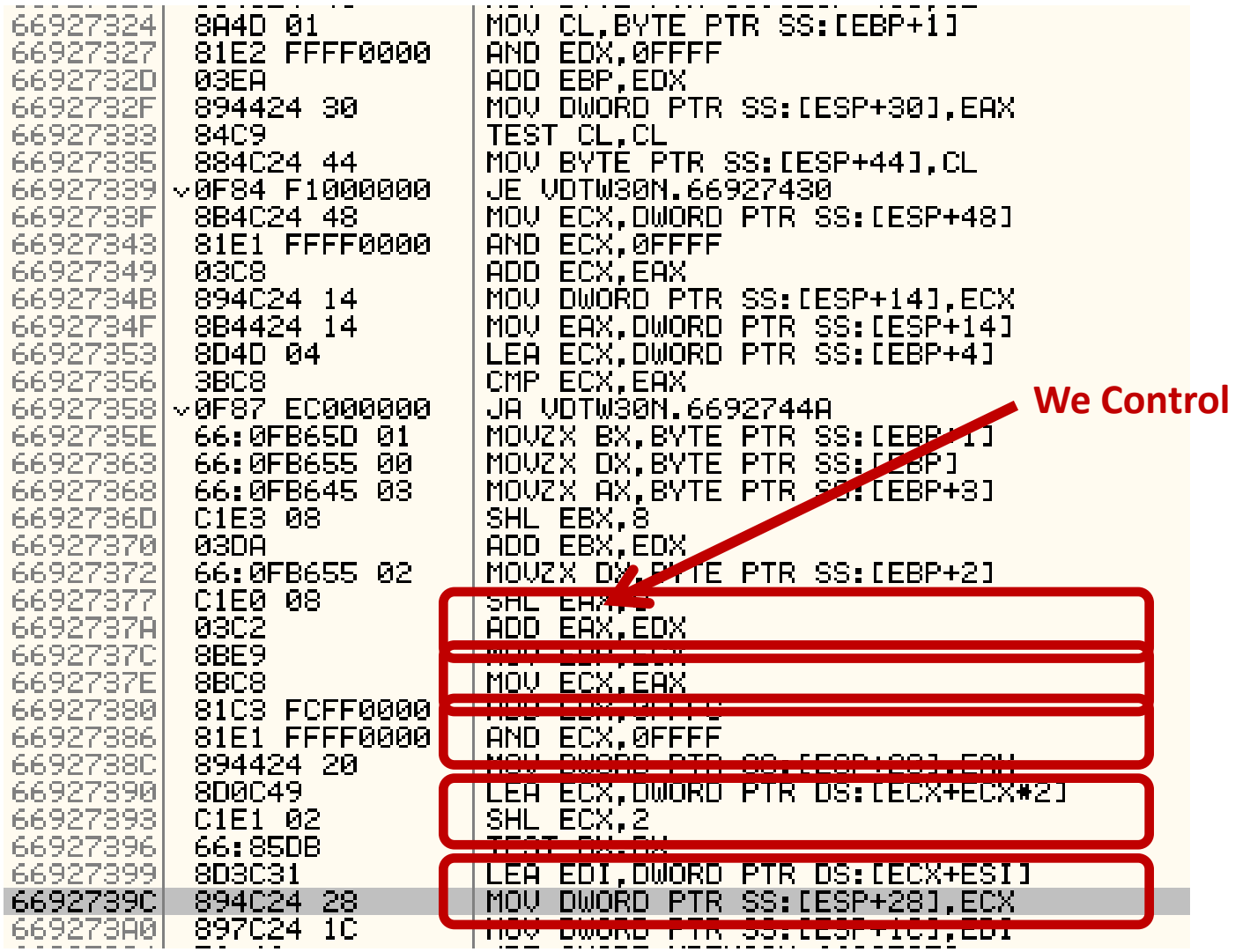
Example Citrix ICA Client Bug

- Old, reported February 2008
- Fixed August 2010
- Affected clients on:
  - Windows
  - Mac
  - Linux
  - Solaris
  - Windows Mobile
- Demo on Windows XP SP2

http://support.citrix.com/article/CTX125975

context INFORMATION SECURITY

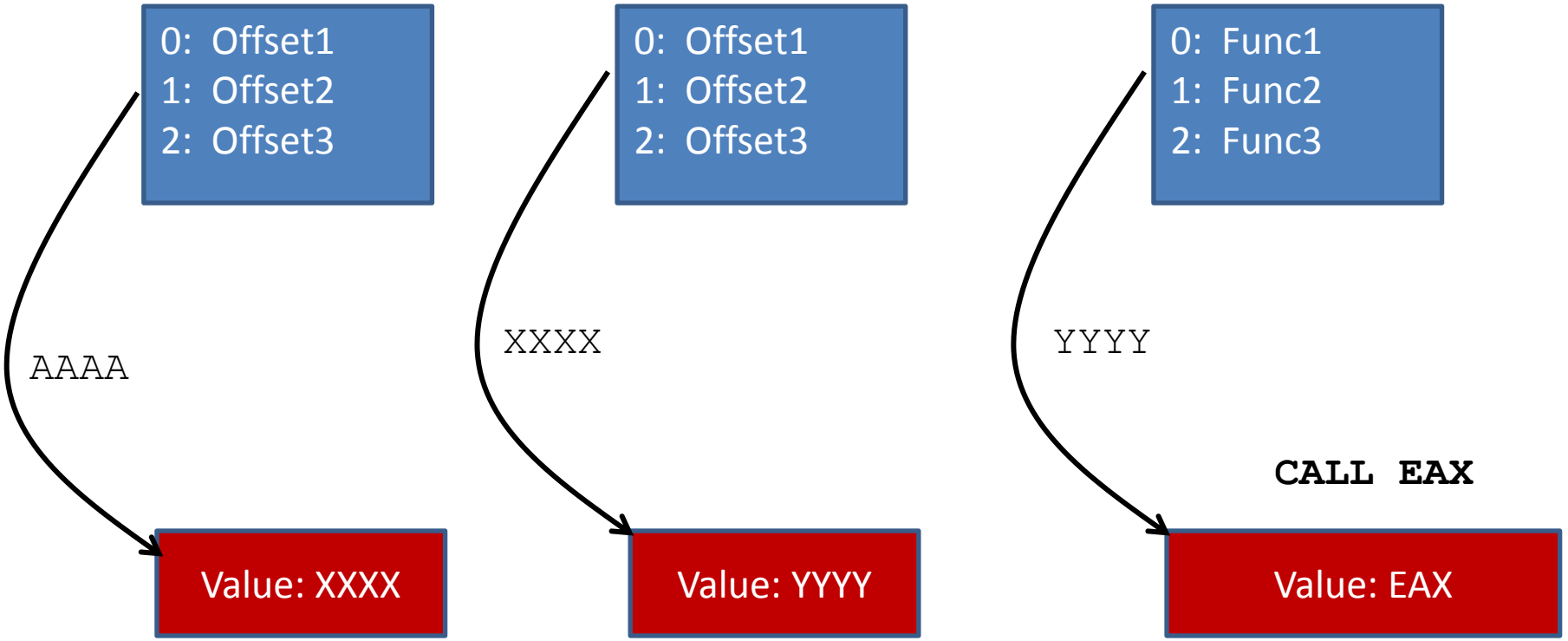

669273DB 8B7C24 1C MOV EDI,DWORD PTR SS:[ESP+1C]
669273DF 8B7424 24 MOV ESI,DWORD PTR SS:[ESP+24]
669273E3 8B4C24 28 MOV ECX,DWORD PTR SS:[ESP+28]
669273E7 EB 05 JMP SHORT VDTW30N.669273EE
669273E9 66:85DB TEST BX,BX
669273EC 75 5C JNZ SHORT VDTW30N.6692744A
669273EE 66:8907 MOV WORD PTR DS:[EDI],AX
669273F1 66:895F 02 MOV WORD PTR DS:[EDI+2],BX
669273F5 66:8B81 C8179366 MOV AX,WORD PTR DS:[ECX+669317C8]
669273FC 66:8947 08 MOV WORD PTR DS:[EDI+8],AX
66927400 8B4C24 2C MOV ECX,DWORD PTR SS:[ESP+2C]
66927404 25 FFFF0000 AND EAX,0FFFF
66927409 C1E0 04 SHL EAX,4
6692740C 8B4408 08 MOV EAX,DWORD PTR DS:[EAX+ECX+8]
66927410 85C0 TEST EAX,EAX
66927412 74 08 JE SHORT VDTW30N.6692741C
66927414 8B5424 3C MOV EDX,DWORD PTR SS:[ESP+3C]
66927418 57 PUSH EDI
66927419 52 PUSH EDX
6692741A FFD0 CALL EAX



context
INFORMATION SECURITY

Offset Value

```
Control Offset:  AAAA
```

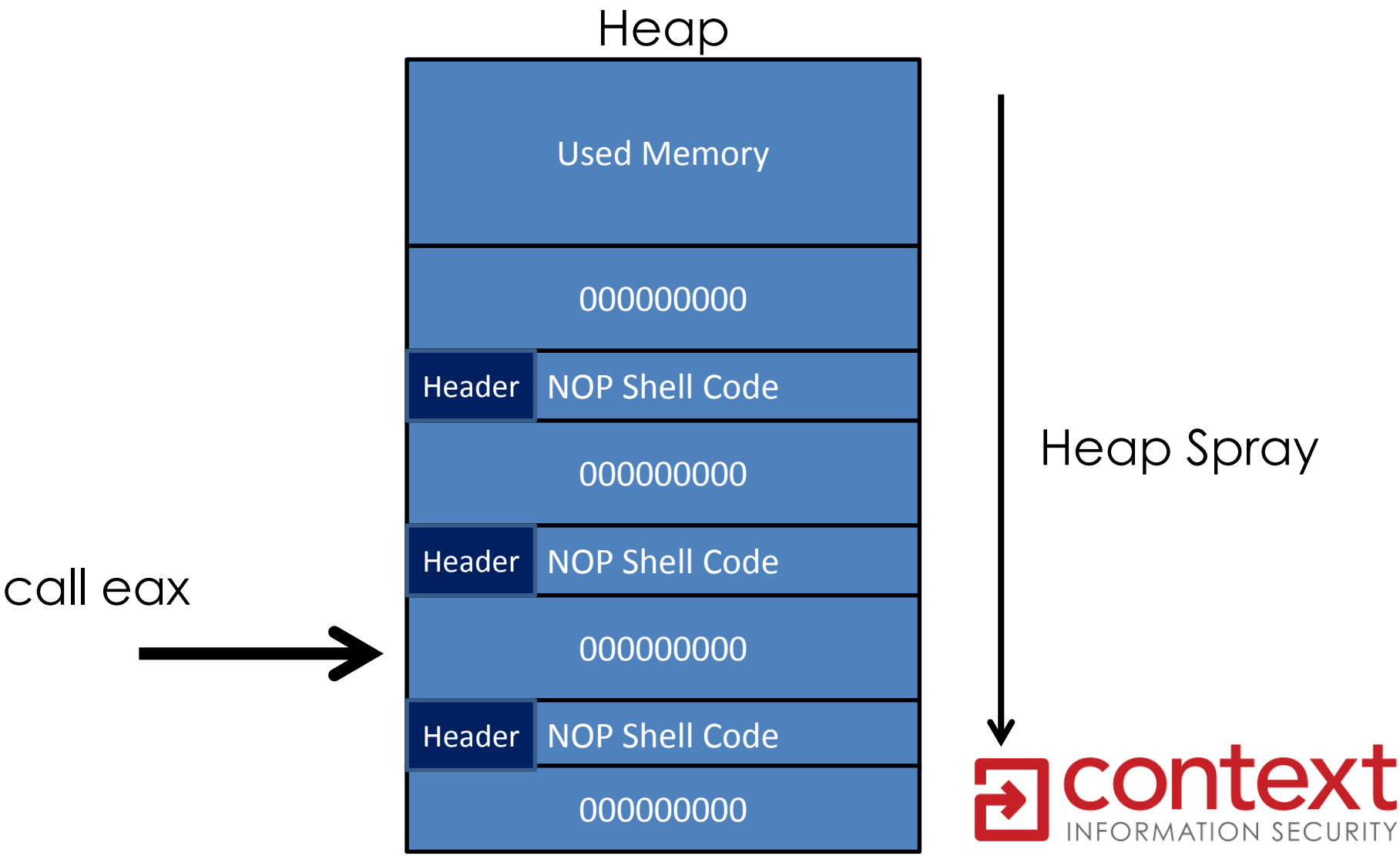


context
INFORMATION SECURITY

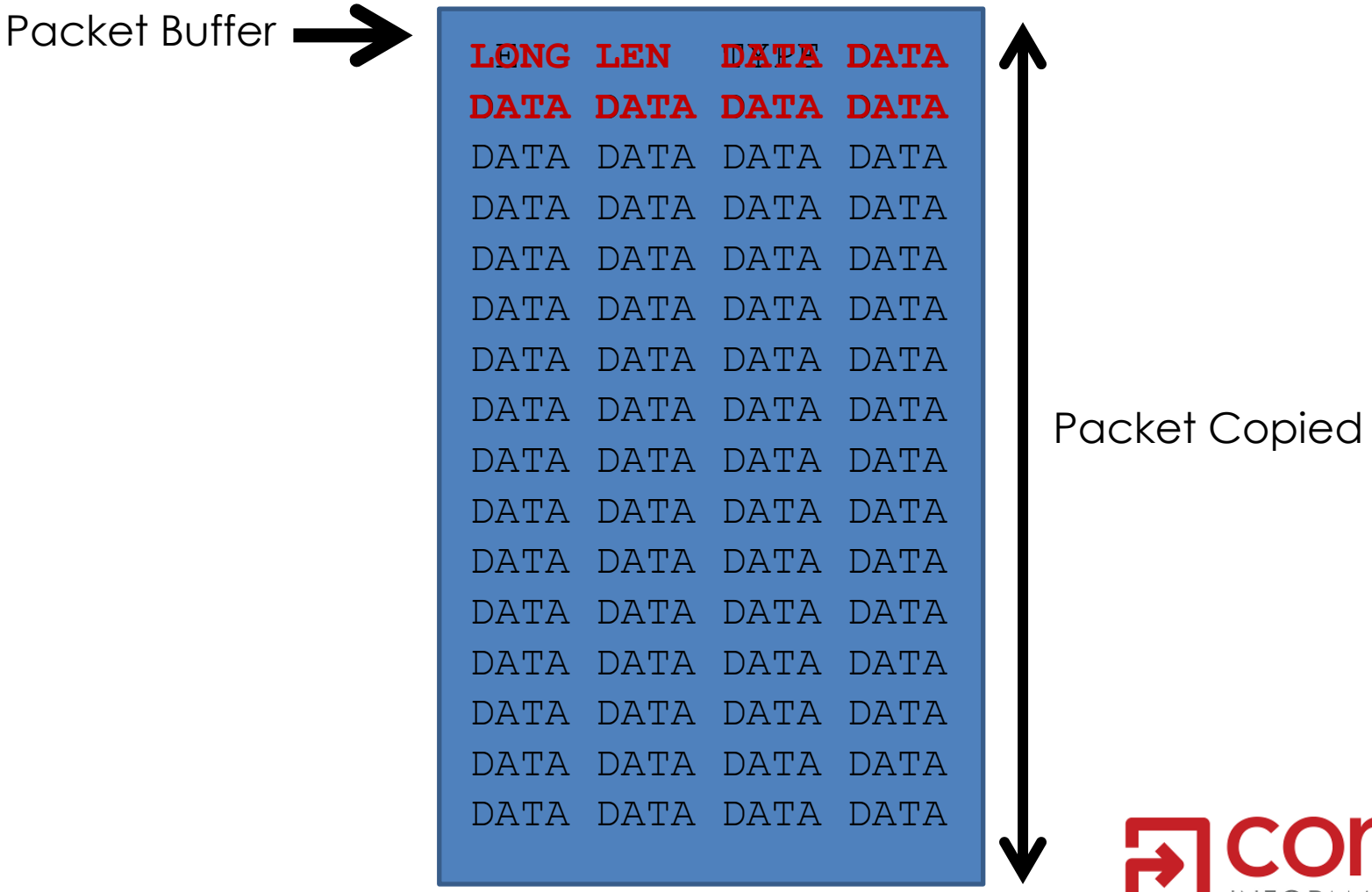
Demo 7

- Brute force the value to find a heap offset

Heap Spray



Easy Heap Spray

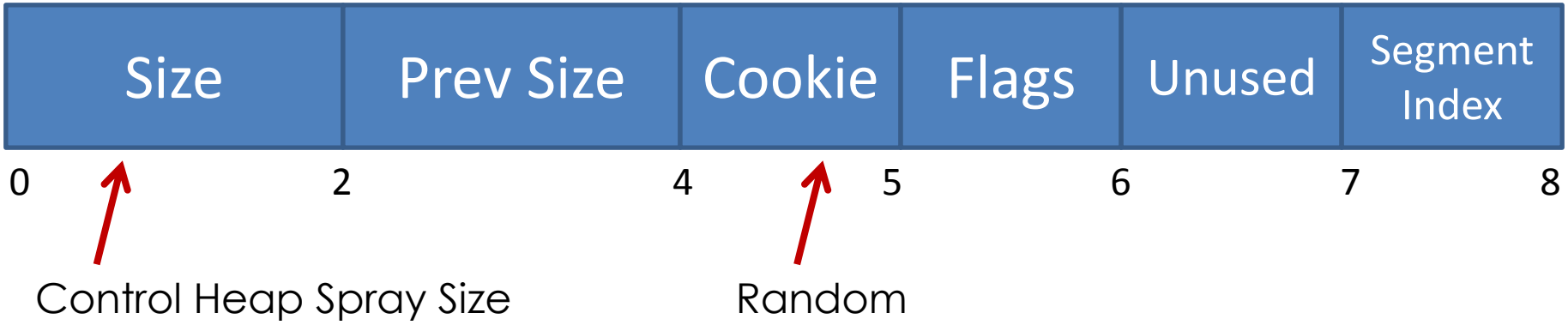


context
INFORMATION SECURITY

Heap Header

Valid Pointer

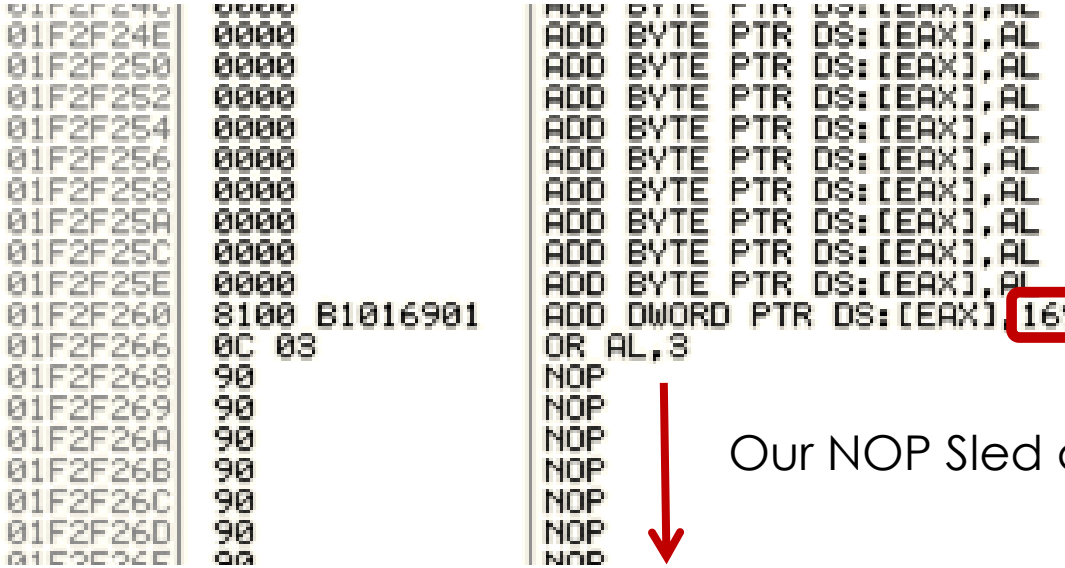
```
0000                    =>              ADD BYTE PTR [EAX],AL
```




```
81 00 =>    ADD DWORD PTR DS:[EAX], PrevSize_Cookie_Flags
```

context
INFORMATION SECURITY

Exec Heap Header



EAX pointer to valid memory

Our NOP Sled and Shellcode

context INFORMATION SECURITY

Demo 8 "Root"

- HTTP send ICA file
- Replay negotiation
- Prime the heap – large packet
- Spray the heap x 5000 – small packet big Len
- Send payload trigger packet

context
INFORMATION SECURITY

Demo 9 "Other Examples"

- The Power of Canape!

Demo 10 "0Day"

- Demo only, sorry ☹

context
INFORMATION SECURITY

Questions

- Please fill in your feedback forms

context
INFORMATION SECURITY

References

- http://canape.contextis.com
- Twitter: @ctxis
- Email: canape@contextis.com

context INFORMATION SECURITY