COSEINC®

Solid Security.Verified.

Industrial Bug Mining

Extracting, Grading and Enriching the Ore of Exploits

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

The Bug Mining Analogy

- Phase 1: Extraction
- Phase 2: Grading
- Phase 3: Enrichment
- Phase 4: ???
- Phase 5: Profit!

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

The Bug Mining Analogy

- Phase 1: Extraction
- Phase 2: Grading
- Phase 3: Enrichment
- Phase 4: ???
- Phase 5: Profit!

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Welcome to the Mt era

- 2009: We use 8 servers to build a virtualised fuzzfarm
  - Sustained testing speed: 30 t/s (2.5Mt / day)
- April 2010: MS describe their ‘fuzzing botnet’
  - “12 million iterations in a weekend” (6Mt/day)
  - Now upwards of 10Mt/d
- May 2010: Project MAN VERSUS BORG!!11! (Bugmine 2.0)
  - Same hardware, complete stripdown and rebuild
  - Test and optimise code / architecture at every step
  - Sustained testing speed: >= 1.12Mt/h

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

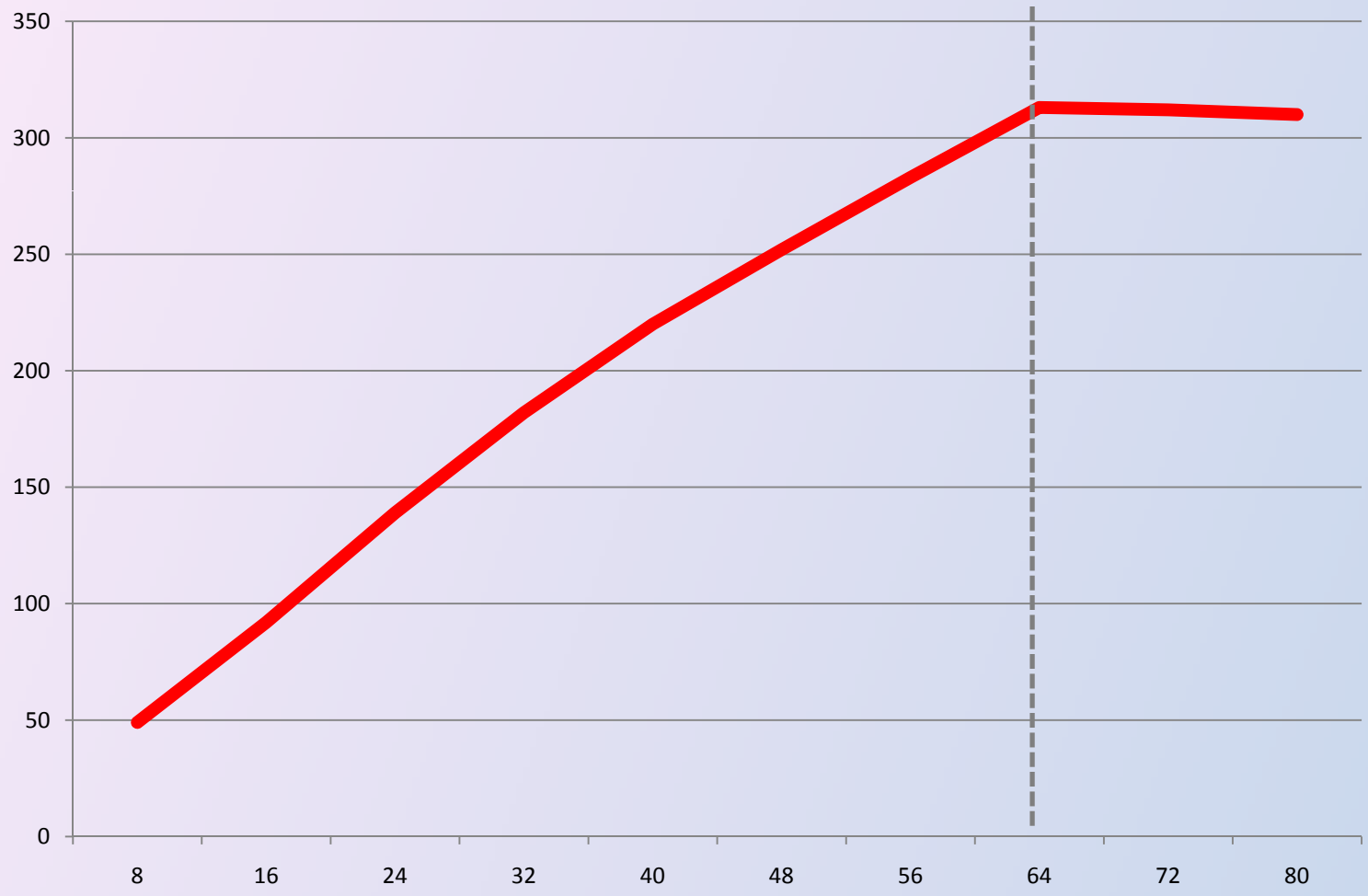
Scale

1. Make each node faster by eliminating bottlenecks
   - network, disk, IO, serialisation, extraneous target code, node OS overhead….
   - You're not doing it right until the last bottleneck is CPU time spent on the real target code
2. When adding new nodes, scale as close to perfectly as possible

Private & Confidential
Property of COSEINC

COSEINC®

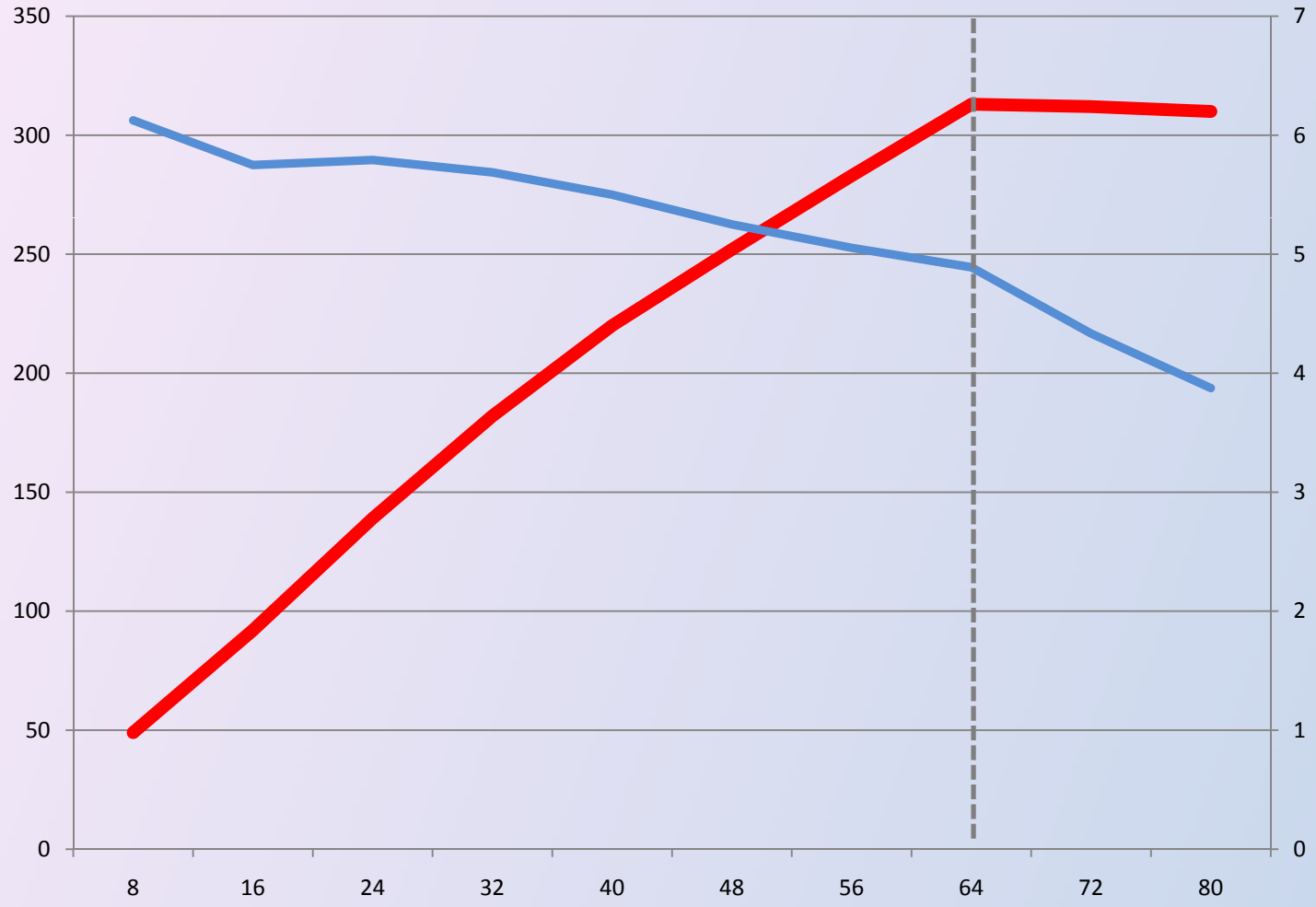
Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Building It

- Switch from ESXi to KVM
  - Real linux, we know how use it
  - Performance is apparently ‘comparable’
- Move storage to a dedicated network
  - Open iSCSI, 4 x 160GB SSD in RAID 0, 4xGigE NIC
  - Oracle Cluster Filesystem (OCFS2) on top
- Optimise Harness
  - Ruby is slow anyway, but I removed the worst problems
- Optimise Fuzzbots
  - Kill explorer.exe for ~15% speedup?!
  - Don’t open a brand new Office process every time

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Building It

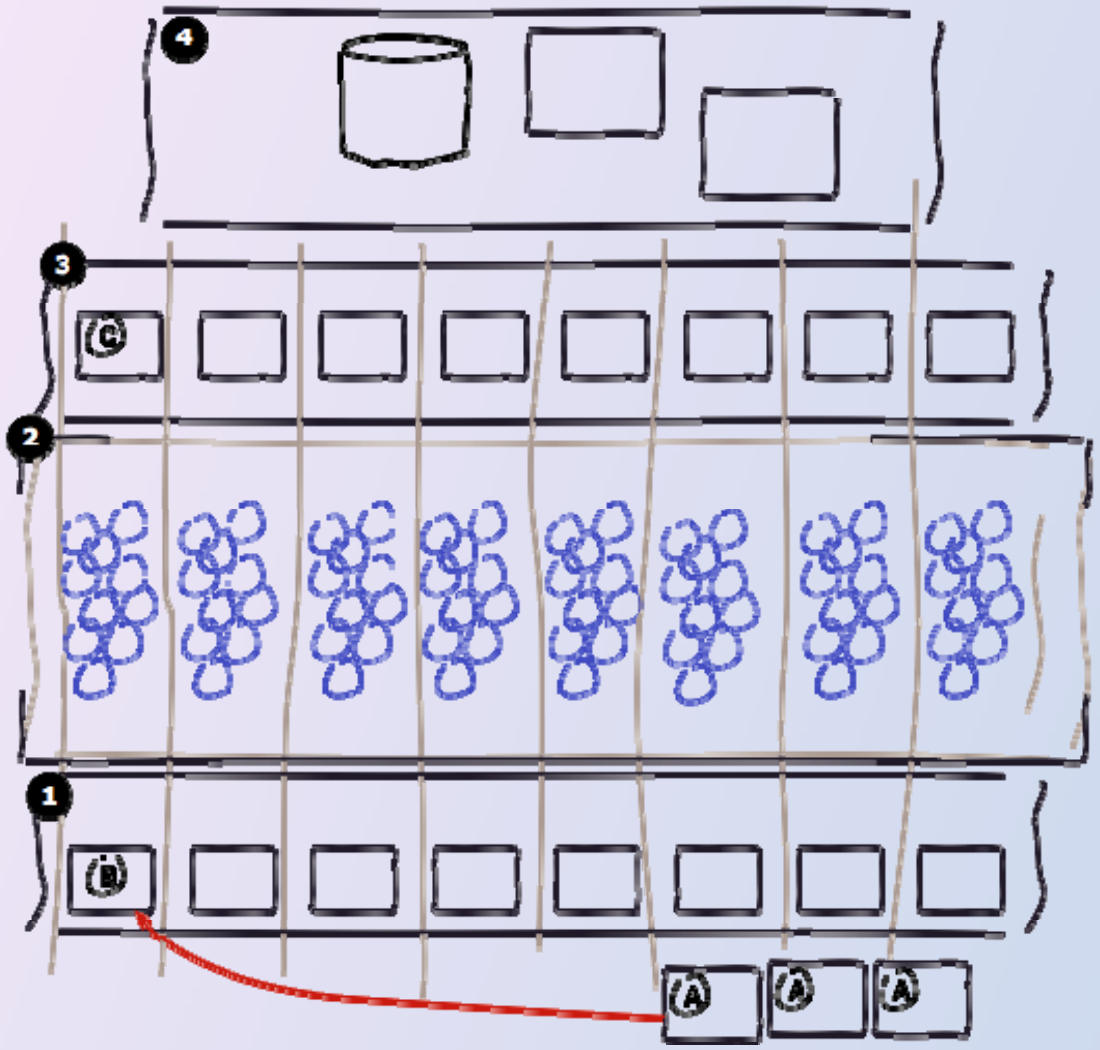
- Easier Provisioning
  - One fuzzbot template
  - Multiple “overlays” (aka “linked clones”)
  - “Snapshot Mode” on top of that
  - Template changes and new rollouts happen in minutes.
- Easier and more powerful management
  - … assuming you like bash and ssh

- Total Software Cost $0 (using MSDN licenses)
- Total Hardware Cost ~ 30k USD

Private & Confidential
Property of COSEINC

COSEINC®

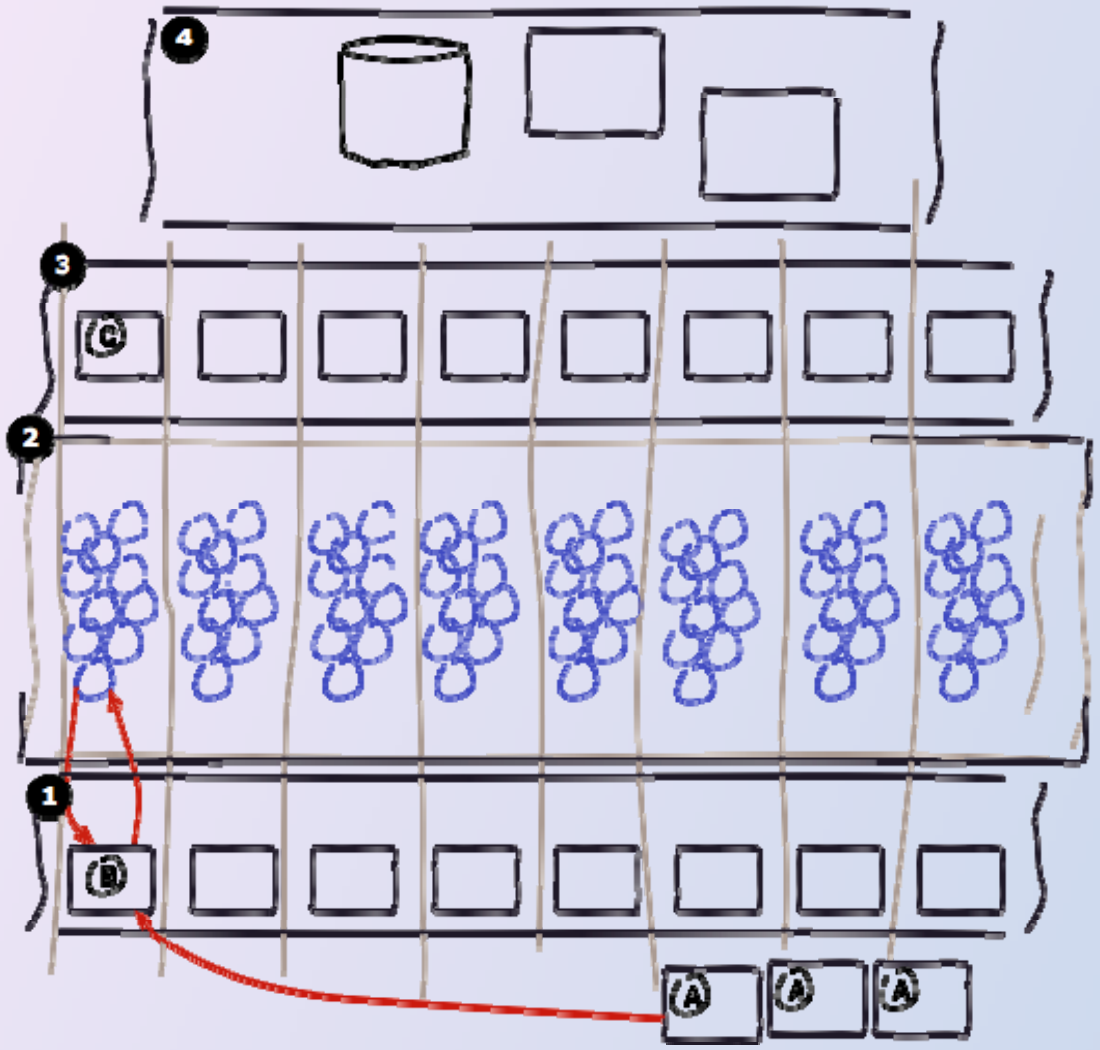
Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

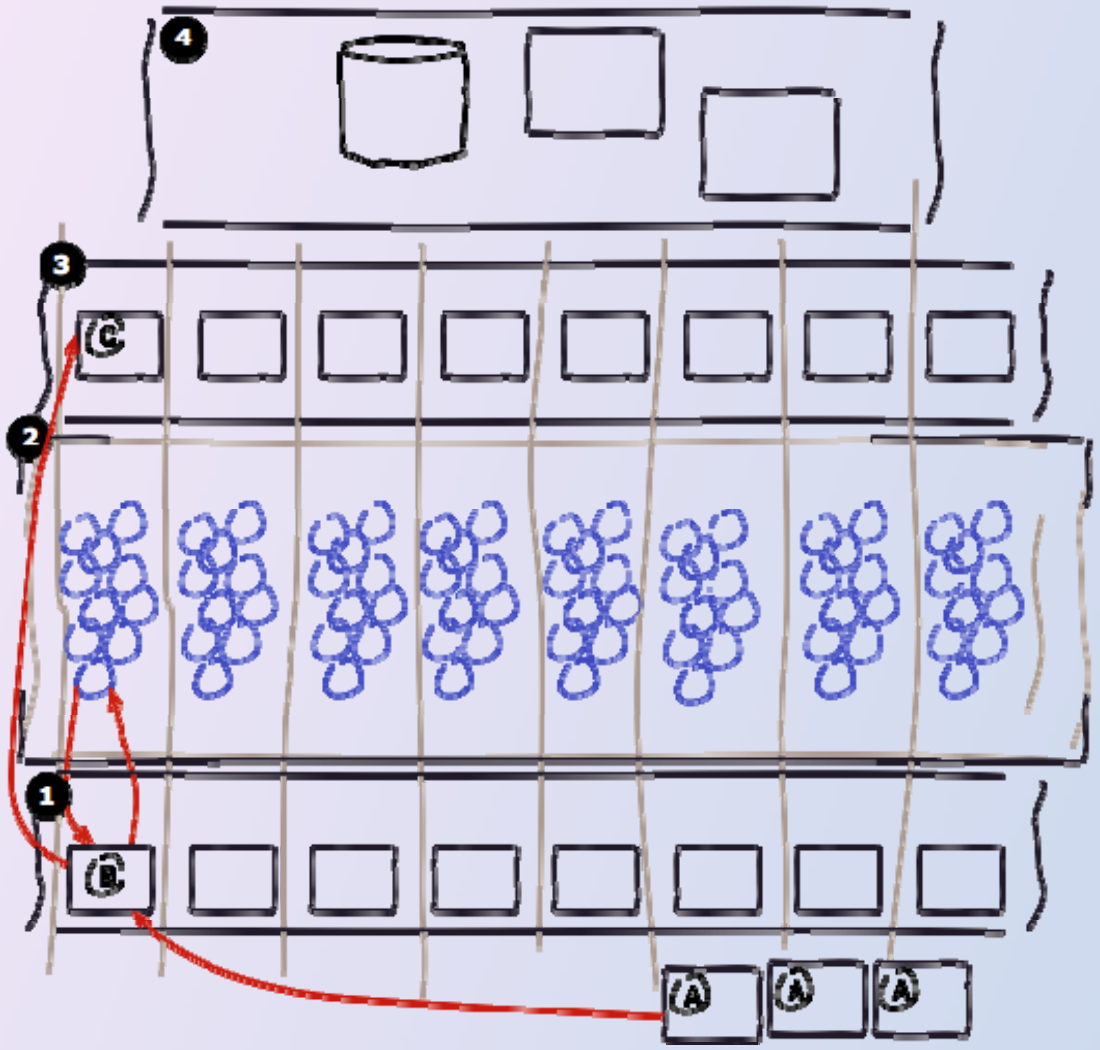
Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

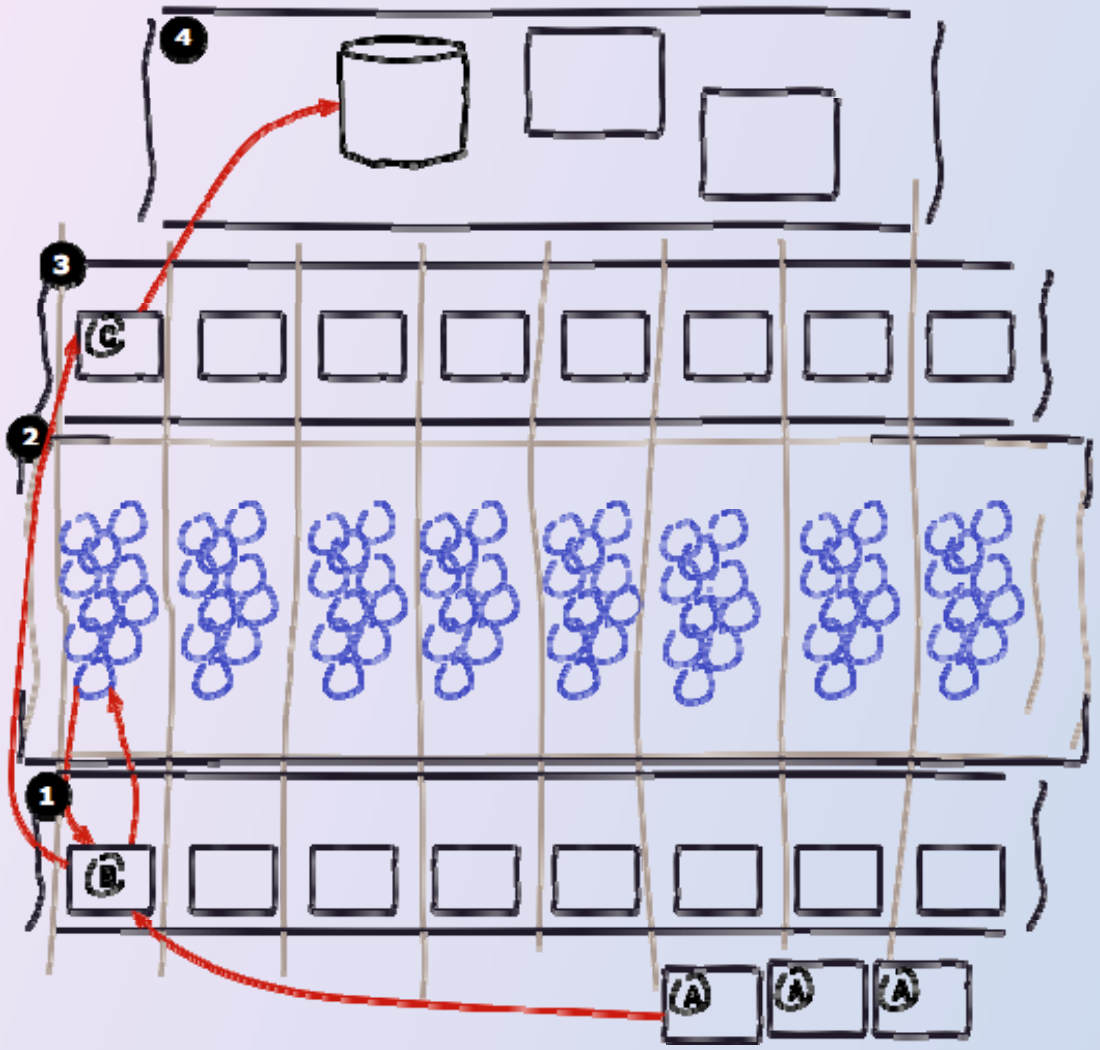
Solid Security. Verified.



Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Features

- Software “Hot swap”
- Tagged queues
- Any DB backend
- Any case producer frontend
- Everything scales horizontally – n producers, n distribution nodes etc etc

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

The Bug Mining Analogy

- Phase 1: Extraction
- Phase 2: Grading
- Phase 3: Enrichment
- Phase 4: ???
- Phase 5: Profit!

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Bug Triage

- There is “exploitable” and EXPLOITABLE.
- !exploitable rocks, but not for this.
- Here are some examples from Word 2007

(X’s will be removed for the show, just for fun)

Private & Confidential
Property of COSEINC

```
head -15 summary.txt
=========SUMMARY===============
<none?>: 229
total: 59965
PROBABLY NOT EXPLOITABLE: 21409
UNKNOWN: 31013
PROBABLY EXPLOITABLE: 6032
EXPLOITABLE: 1282
621 Buckets. 373 unique EIPs.
<none?>: 1
EXPLOITABLE: 88
UNKNOWN: 336
PROBABLY NOT EXPLOITABLE: 86
PROBABLY EXPLOITABLE: 110
================================
```

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Bug Examples

```
--- 0xXXXXXXXX.0xXXXXXXXX (count: 4) ---
EXPLOITABLE: Exploitable - User Mode Write AV starting at
mso!Ordinal7111+0xXXX (Hash=0xXXXXXXXX.0xXXXXXXXX)
XXXXXXX 885e21    mov     byte ptr [esi+21h],bl
ds:0023:32688488=c3
eax=c9330048 ebx=00000000 ecx=32688467 edx=00000000 esi=32688467
edi=00000000 eip=XXXXXXXX esp=001252e8 ebp=001252fc
```

Potentially overwrite a byte with null. Then what?

Private & Confidential
Property of COSEINC

COSEINC

Solid Security.Verified.

Bug Examples

```
--- 0xXXXXXXXX.0xXXXXXXXX (count: 29) ---
PROBABLY EXPLOITABLE: Probably Exploitable - Read Access Violation
on Control Flow starting at wwlib!wdGetApplicationObject+0xXXXXX
(Hash=0xXXXXXXXX.0xXXXXXXXX)
XXXXXXXX ff5028    call    dword ptr [eax+28h]
ds:0023:00000029=????????
eax=00000001 ebx=00000000 ecx=022b6590 edx=00121b1c esi=001218b0
edi=06440000 eip=XXXXXXXX esp=001210d0 ebp=00122140
```

Only awesome if eax is controlled as a 32 bit value…

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Bug Examples

```
--- 0xXXXXXXXX.0xXXXXXXXX (count: 1) ---
EXPLOITABLE: Exploitable - Read Access Violation on Control Flow
starting at wwlib!FMain+0xXXXXX (Hash=0xXXXXXXXX.0xXXXXXXXX)
XXXXXXXX ff5004    call    dword ptr [eax+4]
ds:0023:b4b4b4b8=????????
eax=b4b4b4b4 ebx=00000000 ecx=01f8cf6c edx=0012e6a8 esi=01f8cf6c
edi=06e2366c eip=XXXXXXXX esp=0012e674 ebp=0012e680
```

… like this

Private & Confidential
Property of COSEINC

COSEINC

Solid Security.Verified.

Bug Examples

```
--- 0xXXXXXXX.0xXXXXXXXX (count: 3) ---
PROBABLY NOT EXPLOITABLE: Read Access Violation near NULL starting
at wwlib!DllGetLCID+0xXXX (Hash=XXXXXXXX.0xXXXXXXXX)
XXXXXXXX d7          xlat    byte ptr [ebx]      ds:0023:00000000=??
eax=00120000 ebx=00000000 ecx=01efff68 edx=0012ca20 esi=01ef9568
edi=07971bec eip=XXXXXXXX esp=01efa093 ebp=fff501f8
3213a302 xlat byte ptr [ebx]
3213a303 std
3213a304 fdivr st,st(5)
3213a306 fscale
```

!exploitable fail

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Bug Examples

```
eax=00000000 ebx=00000000 ecx=07a4e008 edx=07a4e440
esi=07a4e43c edi=00000003 eip=07a4e000 esp=0012f650
ebp=0000000d iopl=0          nv up ei pl zr na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000
efl=00010246
07a4e000 0000              add     byte ptr [eax],al
ds:0023:00000000=??
EVENT:DEBUG_EVENT_EXCEPTION
e06d7363 Exception in winext\msec.dll.exploitable debugger
extension.
      PC: 7c812afb  VA: 0006d098  R/W: 19930520  Parameter:
10026bfc
```

EPIC !exploitable fail

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Bug Examples

```
--- 0xXXXXXXXX.0xXXXXXXXX (count: 1) ---
EXPLOITABLE: Exploitable - Read Access Violation at the
Instruction Pointer starting at Unknown Symbol @ 0x0
01010101 ??  ???
eax=06510000 ebx=0012dc14 ecx=064f56a8 edx=00000000 esi=001297cc
edi=00000000 eip=01010101 esp=00125320 ebp=00129724
```

!exploitable needs a new ‘KACHING’ classification

But crashes that cool must be rare, right?

Private & Confidential
Property of COSEINC

COSEINC

Solid Security. Verified.

Not so much…

```
125 eip=00000000
22 eip=00000001
7 eip=00000002
5 eip=00000003
1 eip=00000007
2 eip=00000008
1 eip=0000000c
4 eip=0000000e
4 eip=00000014
1 eip=00000015
2 eip=00000067
1 eip=0000006f
1 eip=00000070
1 eip=00000086
2 eip=00000101
1 eip=00000181
1 eip=00000225
2 eip=00000300
2 eip=00000b33
1 eip=00001571
1 eip=00001733
1 eip=0000671d
2 eip=00006887
1 eip=00008201
9 eip=0000c084
1 eip=0000da66
1 eip=0000db01
3 eip=00320031
1 eip=00380032
29 eip=004001b8
20 eip=004002b8
1 eip=0044002e
1 eip=00510005
1 eip=0061004c
2 eip=00640072
4 eip=00650069
5 eip=00650074
1 eip=00690046
1 eip=00690053
1 eip=006c0070
1 eip=006e0065
1 eip=006f002e
2 eip=006f0068
1 eip=0070006f
1 eip=00720063
2 eip=00740069
1 eip=006e0065
1 eip=006f002e
2 eip=006f0068
1 eip=0070006f
1 eip=00720063
2 eip=00740069
4 eip=01010101
1 eip=01040101
1 eip=04000000
4 eip=04010101
1 eip=04030100
4 eip=04850f49
2 eip=04c25d5e
1 eip=0a09007c
2 eip=0f800000
1 eip=14065a00
1 eip=16010273
1 eip=249f009a
1 eip=277f00fa
228 eip=2a680531
1 eip=40180000
1 eip=42c2fea9
1 eip=43003d00
3 eip=458b50ff
2 eip=507e8068
2 eip=56ec8b55
4 eip=575c302e
1 eip=60010006
2 eip=65747369
2 eip=676e6964
1 eip=6f6c6f43
6 eip=776f6853
1 eip=80000001
1 eip=8bec8b55
1 eip=90909090
1 eip=b0202fd0
4 eip=b4b4b4b4
357 eip=c13b0000
1 eip=c240c033
5 eip=c3321204
5 eip=c3efa5c3
1 eip=f7c88b08
1 eip=f98b5733
1 eip=ff010274
2 eip=ff8f4aa3
1 eip=ff8f4b29
2 eip=ffffffff
```

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

The Bug Mining Analogy

- Phase 1: Extraction
- Phase 2: Grading
- Phase 3: Enrichment
- Phase 4: ???
- Phase 5: Profit!

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Curse you, Aitel!

"Take each basic block and number it. Execute the program twice, once with your crashing file, and once with your template. This generates two signals, which have a stream of numbers in them (from the execution trace). Then you can do interesting things[…]"

-- Dailydave ML, 6/8/09

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Curse you, Aitel!

"I'm not sure what the interesting thing here is that magically tells you something is worth really digging into? Maybe you take your two signals, and subtract their frequencies and visualize how different they are? Throw that at a HMM/NN and make it tell you something?"

-- Dailydave ML, 6/8/09

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Step 0 - Runtrace

- We used DynamoRIO
- VERY fast, kind of a pain in the butt to work with
- Our call tracer is pretty much a “hello world” plugin
- Getting it to make took way longer than writing the code
- (All the runtrace side was written by The Grugq)

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

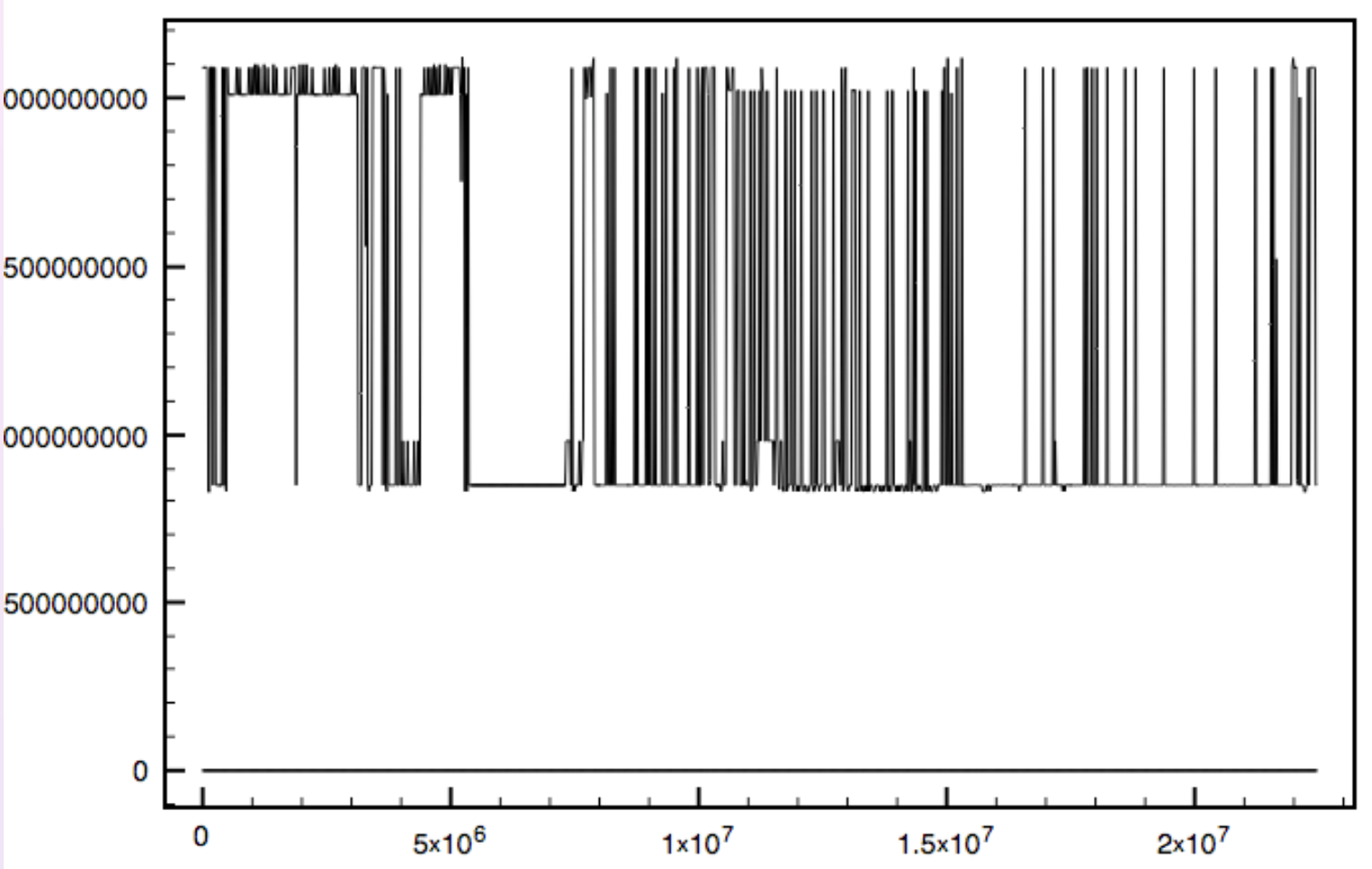
Problems

- The ‘streams of numbers’ are really long
- Visualisation turned out not to be useful
- FFT and HMM etc were red herrings
- NN is buzzword bingo
- We could just use diff, if we could work out a way to make the sequences small enough….

Private & Confidential
Property of COSEINC

COSEINC®

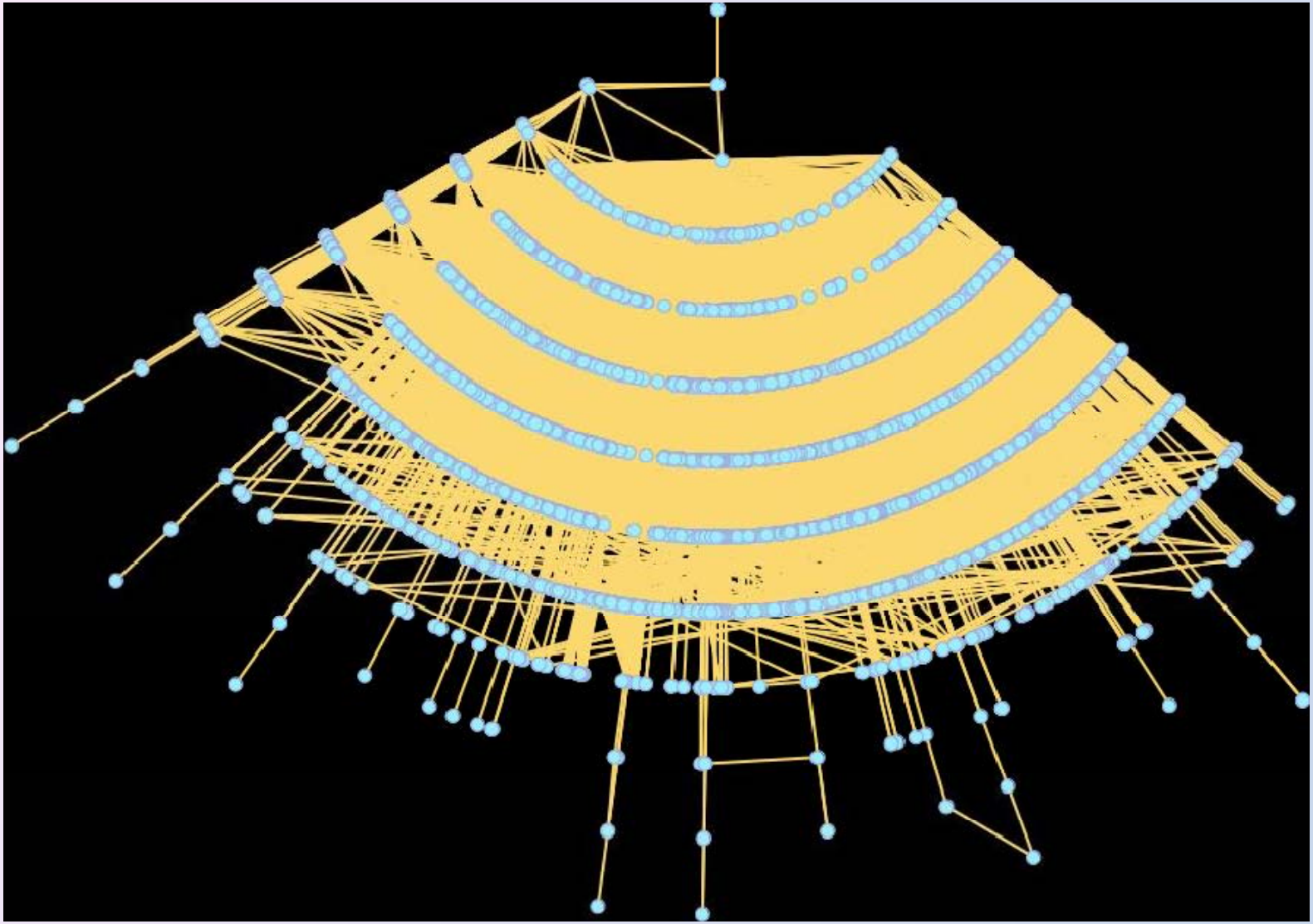
Solid Security.Verified.



Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.



Property of COSEINC

COSEINC®

Solid Security.Verified.

Heirarchical Grammars

pease porridge hot

pease porridge cold

pease porridge in the pot

nine days old

some like it hot

some like it cold

some like it in the pot

nine days old

The SEQUITUR Algorithm
http://sequitur.info/
Written by
Craig Nevill-Manning, Rutgers University,
Ian Witten, University of Waikato, New Zealand

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

0 -> 1 2 3 4 3 5 6 2 6 4 6 5 \n

1 -> p e a s 7 r r i d g 8

2 -> h o t

3 -> \n 1

4 -> c 9

5 -> 10 _ t h 7 t \n n 10 8 d a y s _ 9

6 -> \n s o m 8 l i k 8 i t _

7 -> 8 p o

8 -> e _

9 -> o l d

10 -> i n

The SEQUITUR Algorithm
http://sequitur.info/
Written by
Craig Nevill-Manning, Rutgers University,
Ian Witten, University of Waikato, New Zealand

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Problems

- The grammar is generated on the fly, so different files will generate different grammars
- Wrote a ‘recompressor’
  - Convert the grammar to a ‘Trie’
  - Use the Trie to apply a selected grammar to a selected sequence

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

The approach

- Take transitions addrA ->addrB
- Store in a DB, use the tuple index as sequence elements
- Recompress the original and variant TIS
- Diff
- Post process the diff to add some interesting info

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Annoying, hard to read green screen demo…

Private & Confidential
Property of COSEINC

COSEINC®

Solid Security.Verified.

Beer!

But questions may be asked first.

ben at coseinc dot com

Private & Confidential
Property of COSEINC