BareCloud:
Bare-metal Analysis-based Evasive Malware Detection

Dhilung Kirat, Giovanni Vigna, Christopher Kruegel

UC Santa Barbara

USENIX Security 2014

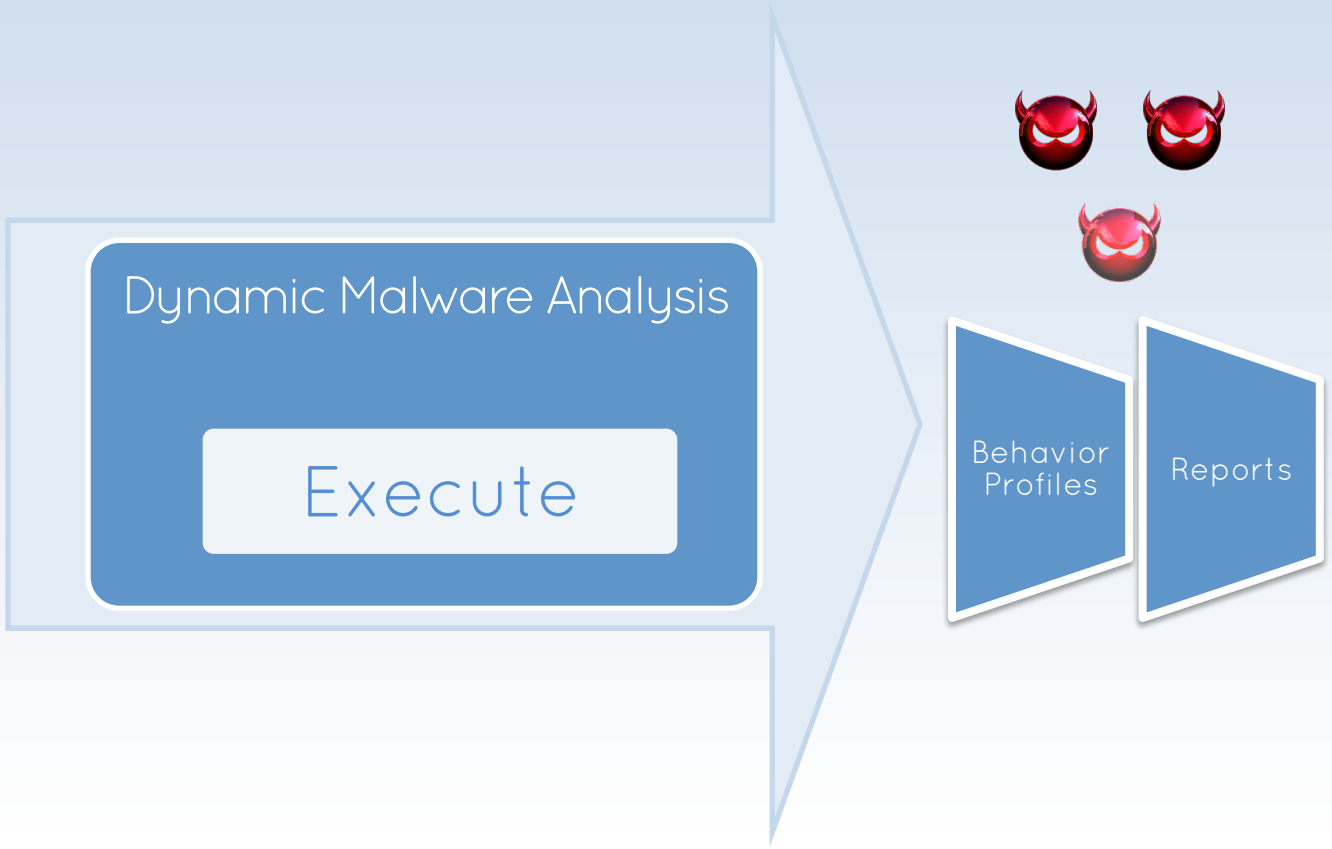
San Diego, CA

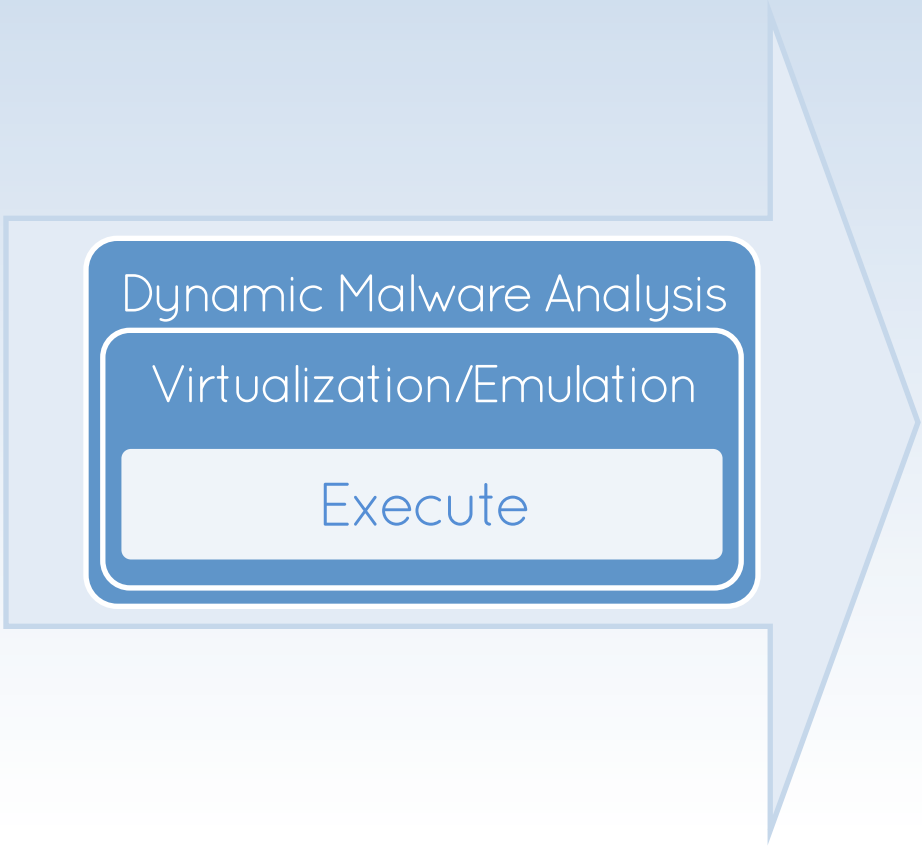
Dynamic Malware Analysis

Execute

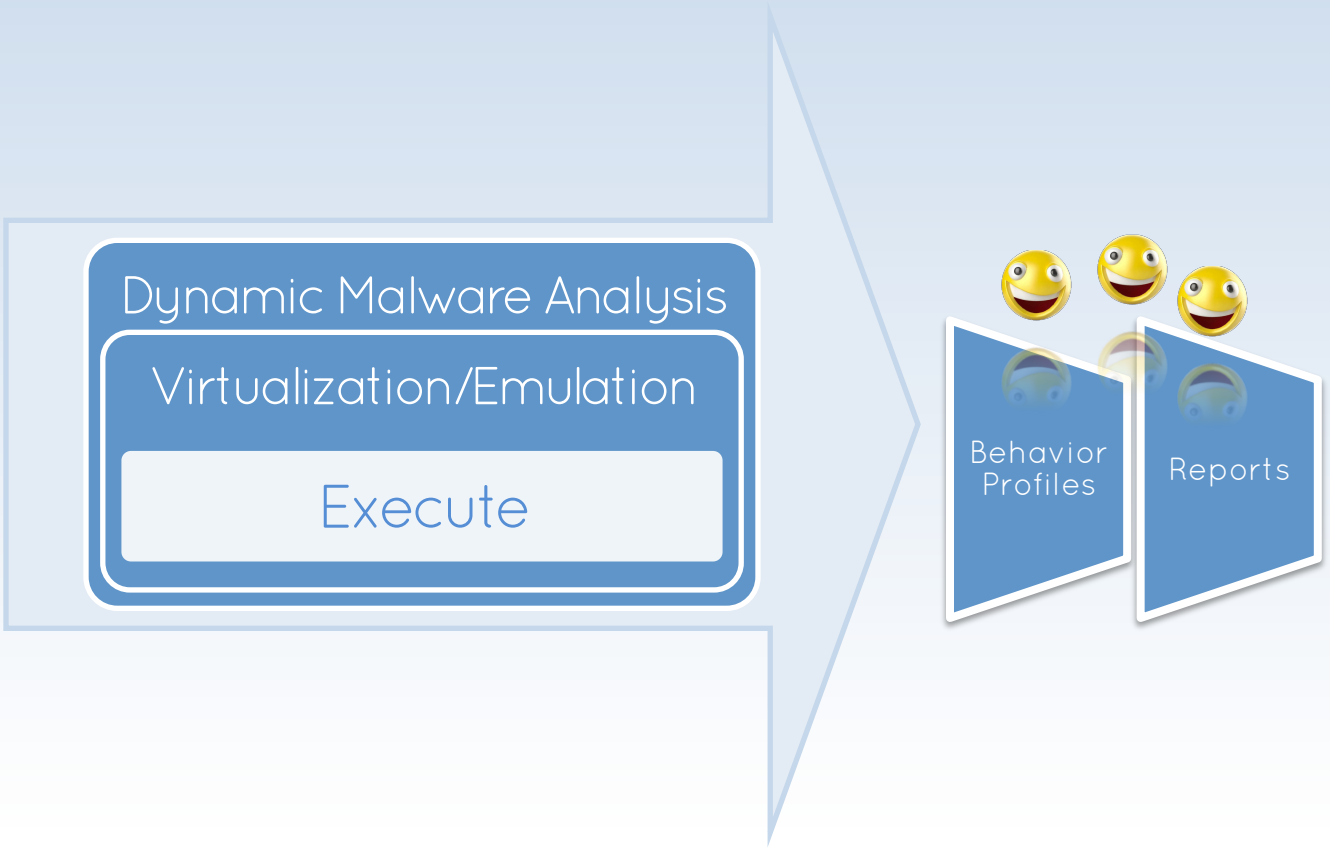
Behavior Profiles

Reports

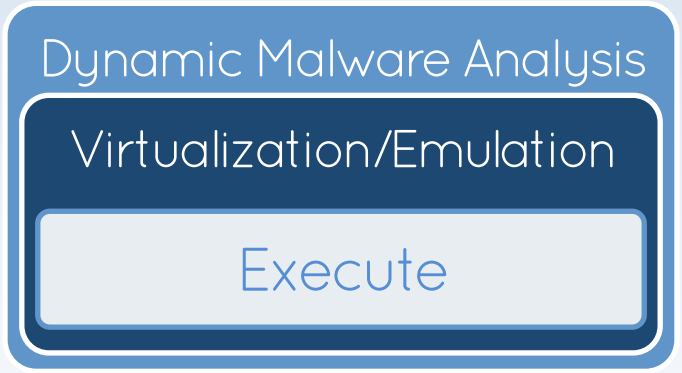

Dynamic Malware Analysis
Execute
Behavior Profiles
Reports


Dynamic Malware Analysis
Virtualization/Emulation
Execute
Behavior Profiles
Reports

Evasive Malware



Evasive Malware



Detect Analysis Environment

- Disk
  - HKLM\Hardware\DeviceMap\Scsi
  - HKLM\System\CurrentControlSet\Services\Disk\Enum
- Bios
  - HKLM\Hardware\Description\System\SystemBiosVersion
- Keyboard/Mouse
  - Presence of mouse, keyboard layout
- User
  - Username, Windows Product ID
  - Active user

Detect Analysis Environment

- CPU
  - SIDT instruction

```
int swallow_redpill () {
  unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";
  *((unsigned*)&rpill[3]) = (unsigned)m;
  ((void(*)())&rpill)();
  return (m[5]>0xd0) ? 1 : 0;
}
```

  - CPU Emulation bug (including MMX instruction set)

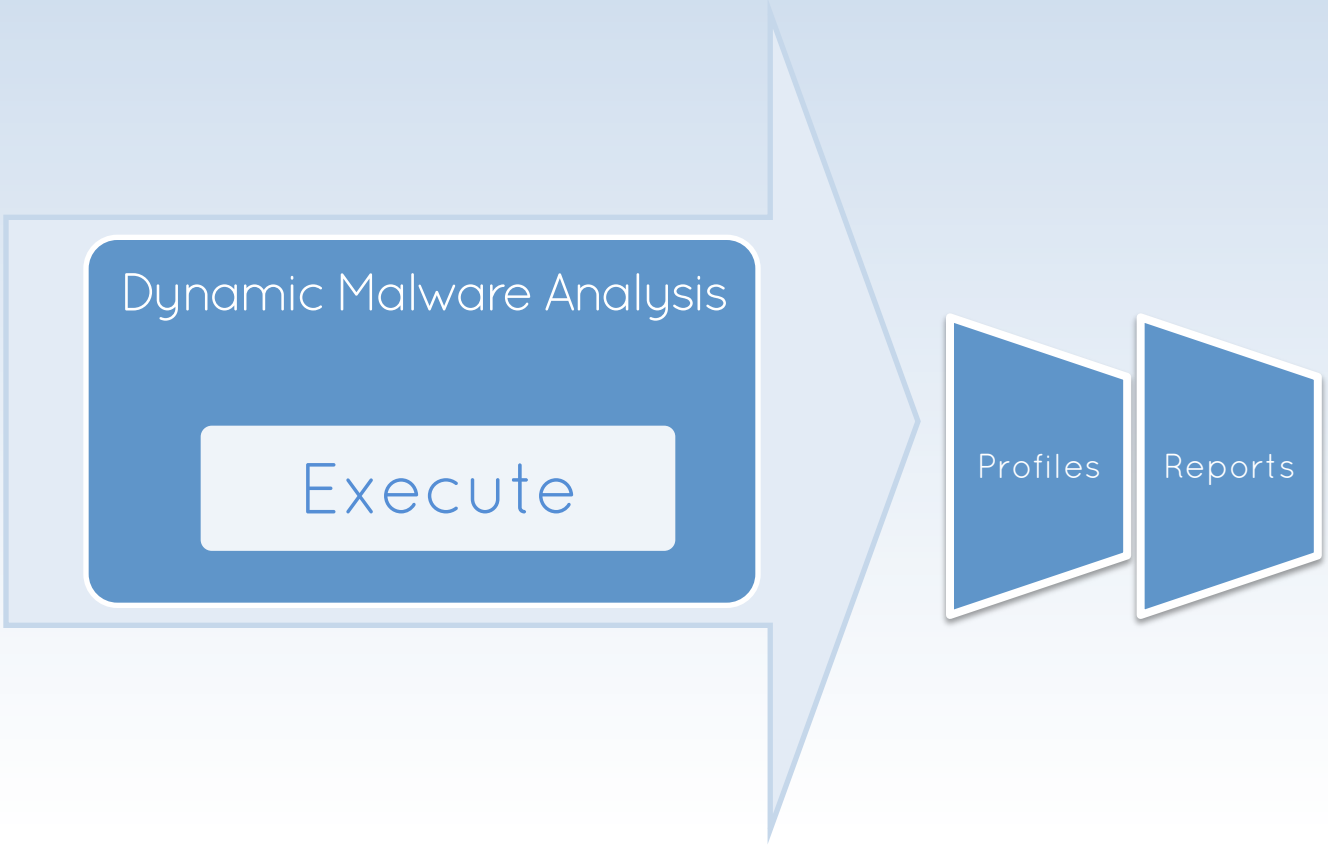
- Vulnerability
  - CVE-2012-3221 VirtualBox

```
int crash() {
  asm (
    "int $0x8;"
    : // output: none
    : // input: none
    :"%eax", "%ebx", "%ecx", "%edx"    // clobbered register
  );
  return(0);
```

- Timing attack
  - The virtualization and emulation systems add some level of overhead

Fully Undetectable (FUD)

Solutions?



Transparent Analysis

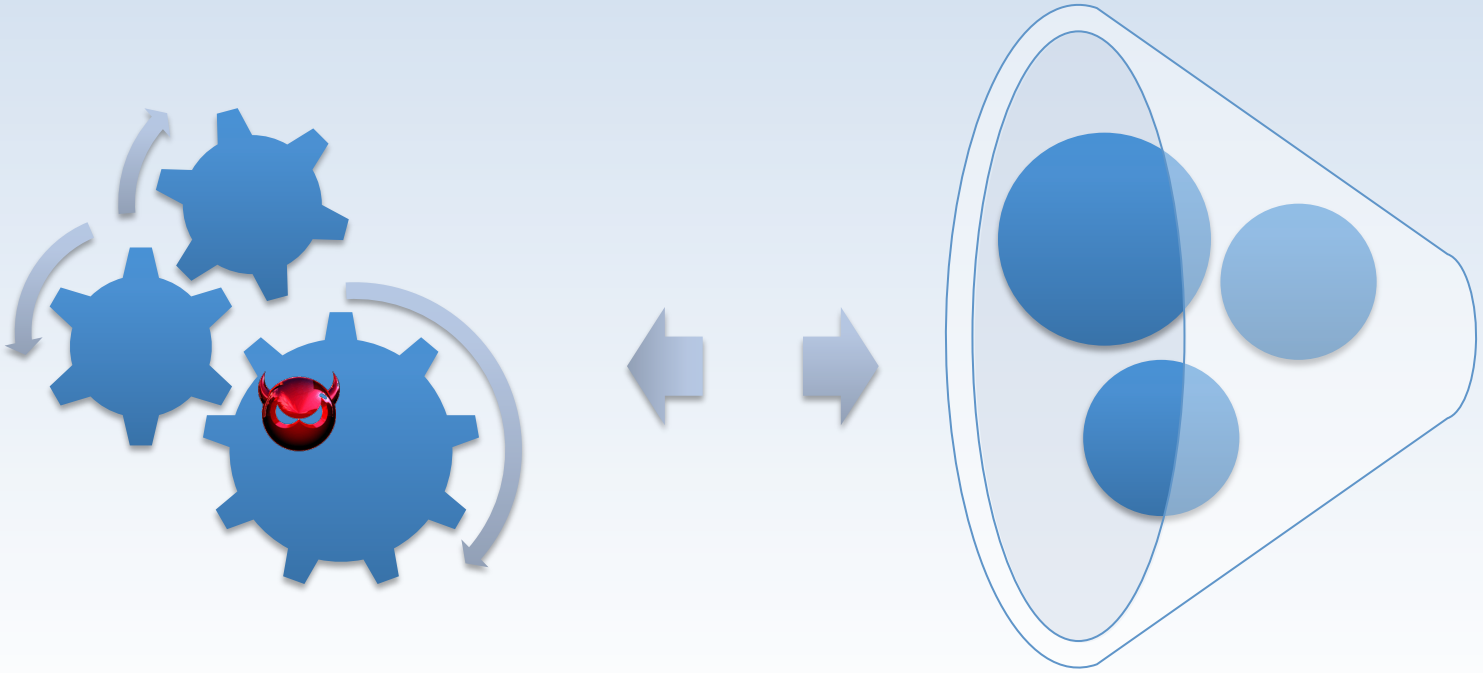
Dynamic Malware Analysis

Execute

Profiles

Reports

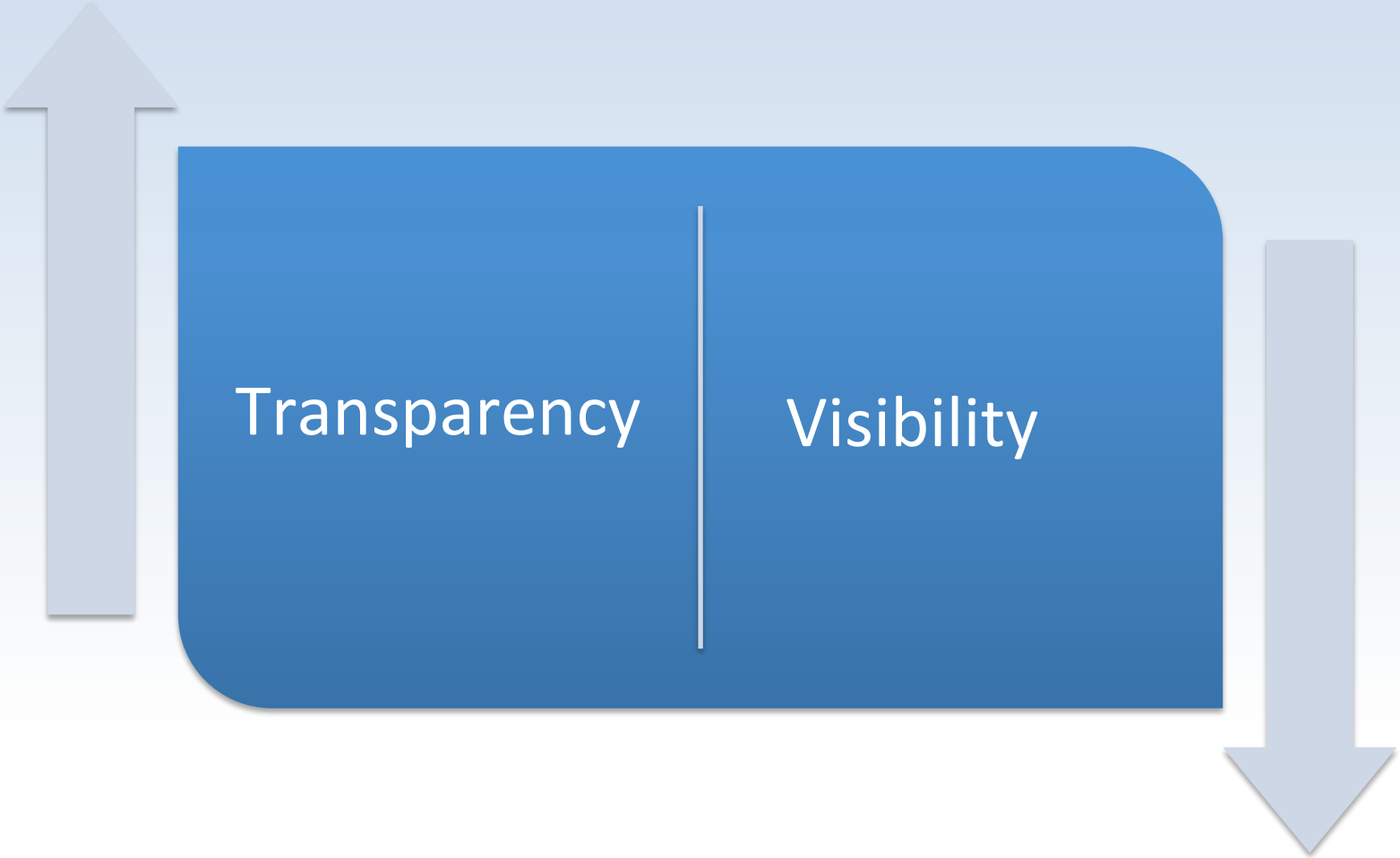
Transparent Analysis



Execution Environment

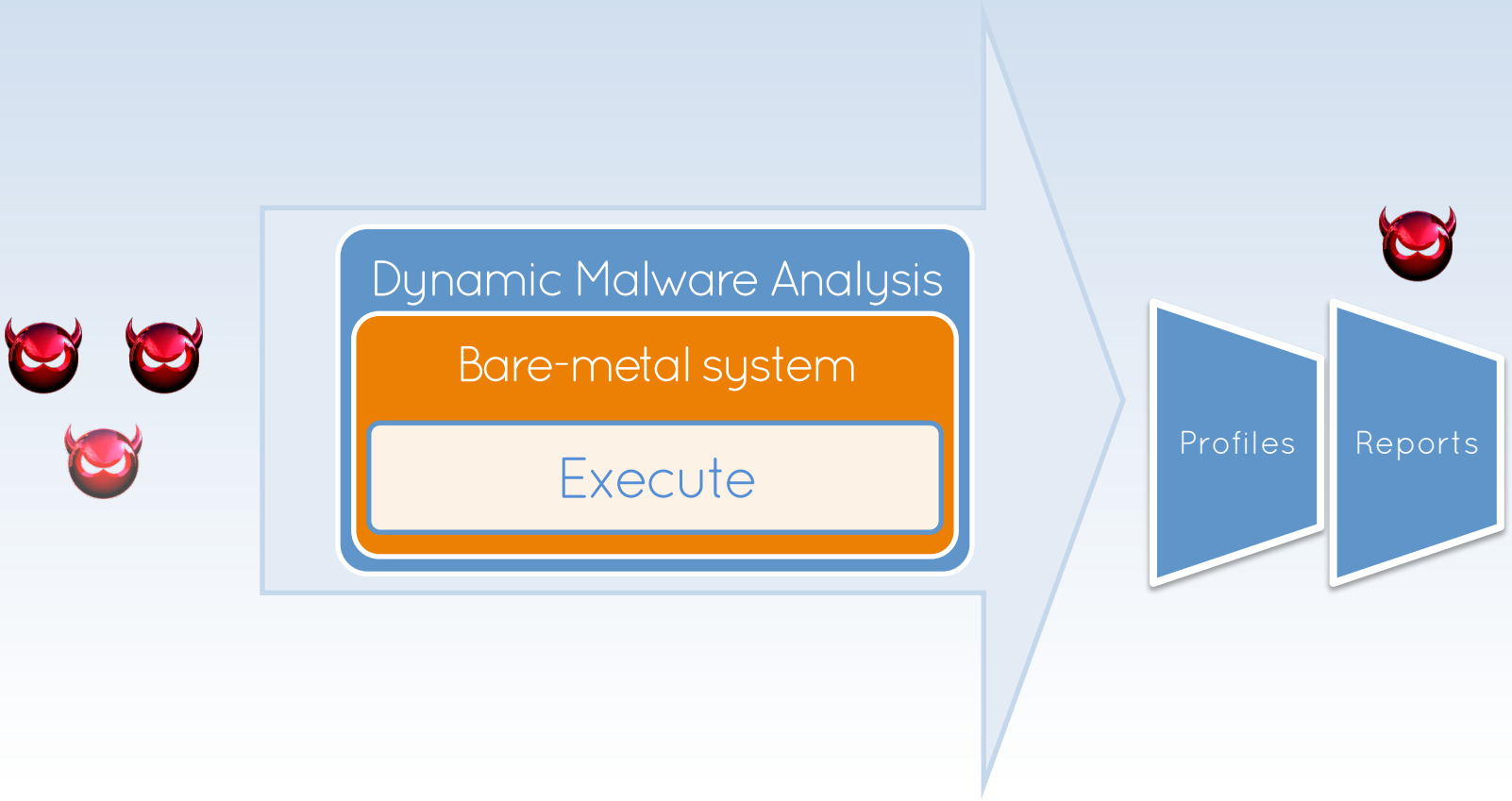
Monitoring Components

Dynamic Malware Analysis

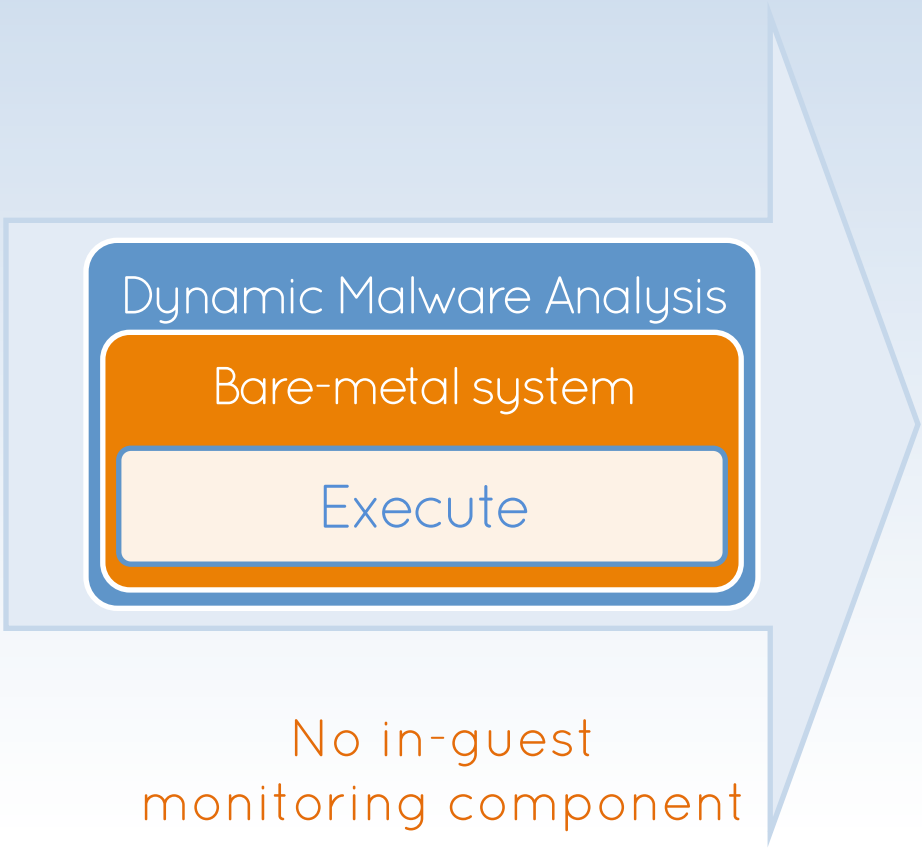


Can we automatically identify evasive malware under reduced visibility?

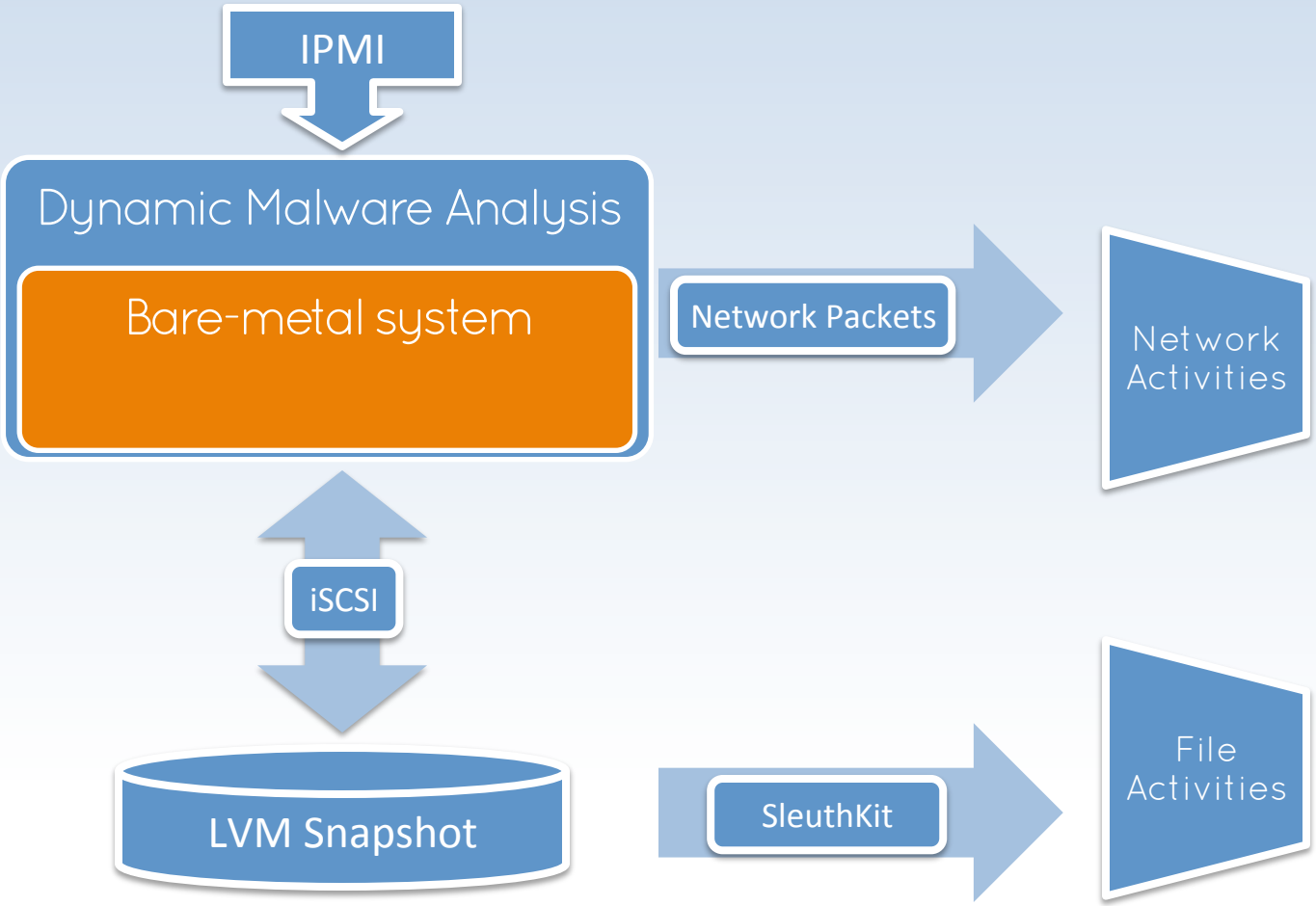
BareCloud


Dynamic Malware Analysis
Bare-metal system
Execute
Profiles
Reports

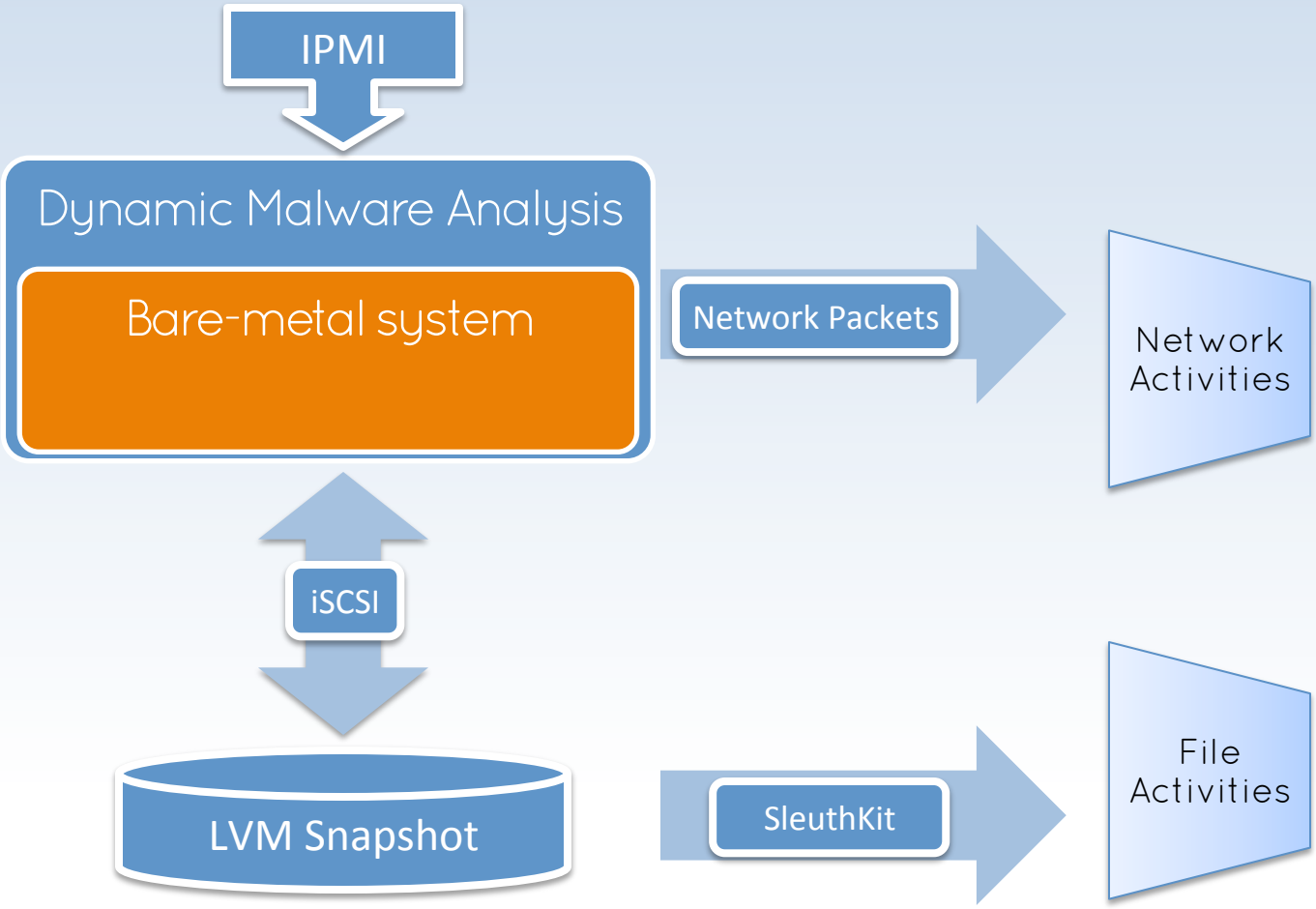
BareCloud


Dynamic Malware Analysis
Bare-metal system
Execute
Profiles
Reports
No in-guest
monitoring component

BareCloud

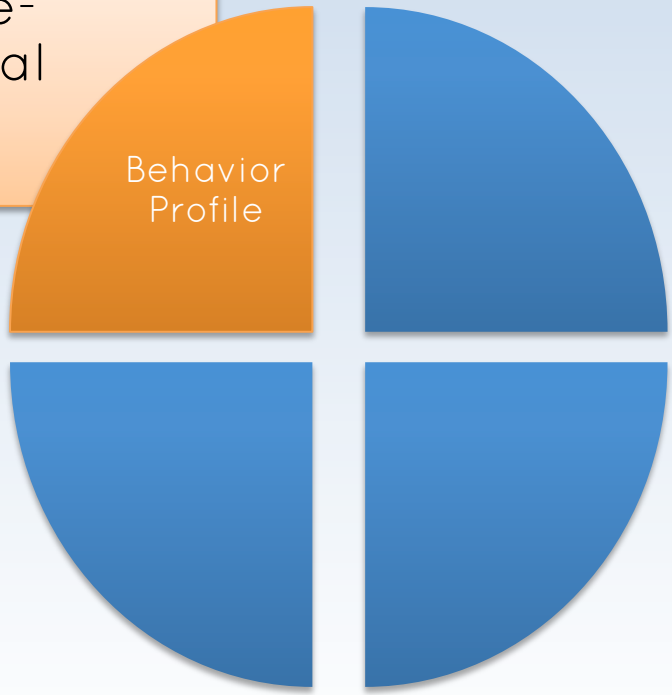

IPMI
Dynamic Malware Analysis
Bare-metal system
Network Packets
Network Activities
iSCSI
LVM Snapshot
SleuthKit
File Activities

BareCloud

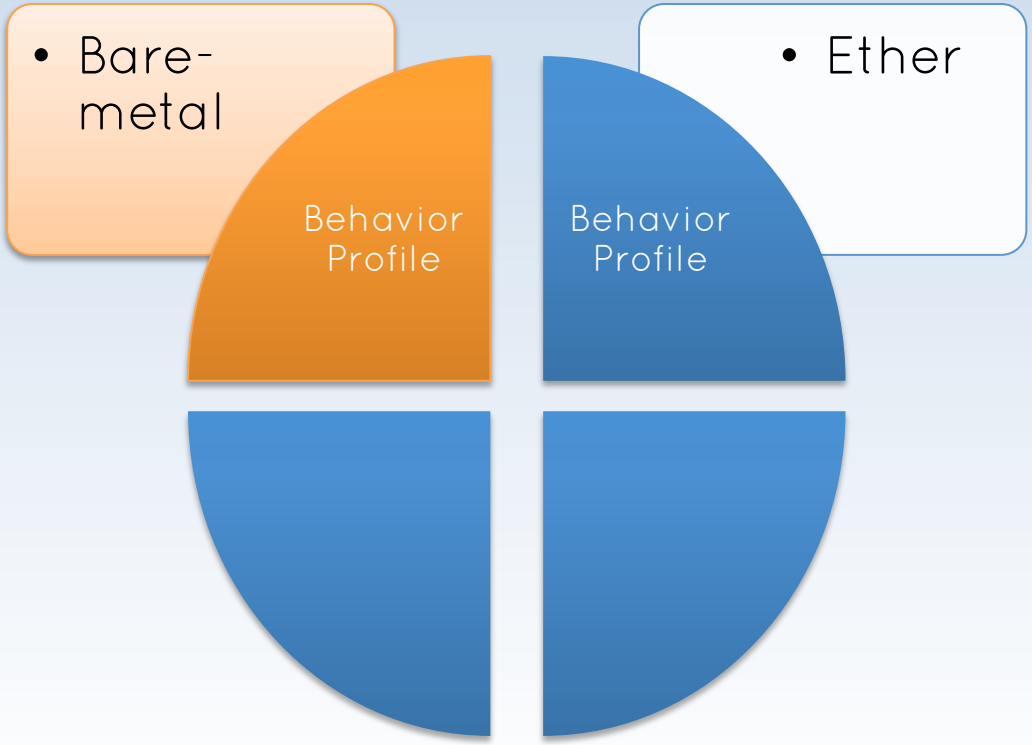

IPMI
Dynamic Malware Analysis
Bare-metal system
Network Packets
Network Activities
iSCSI
LVM Snapshot
SleuthKit
File Activities

BareCloud

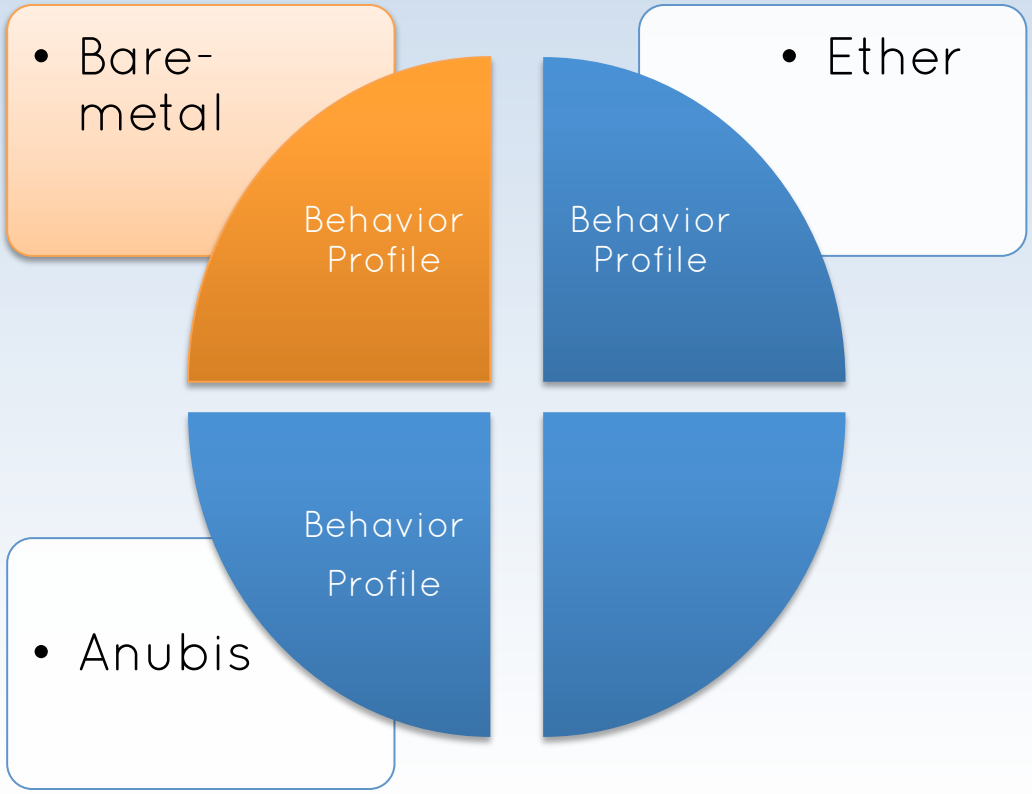
- Bare-metal



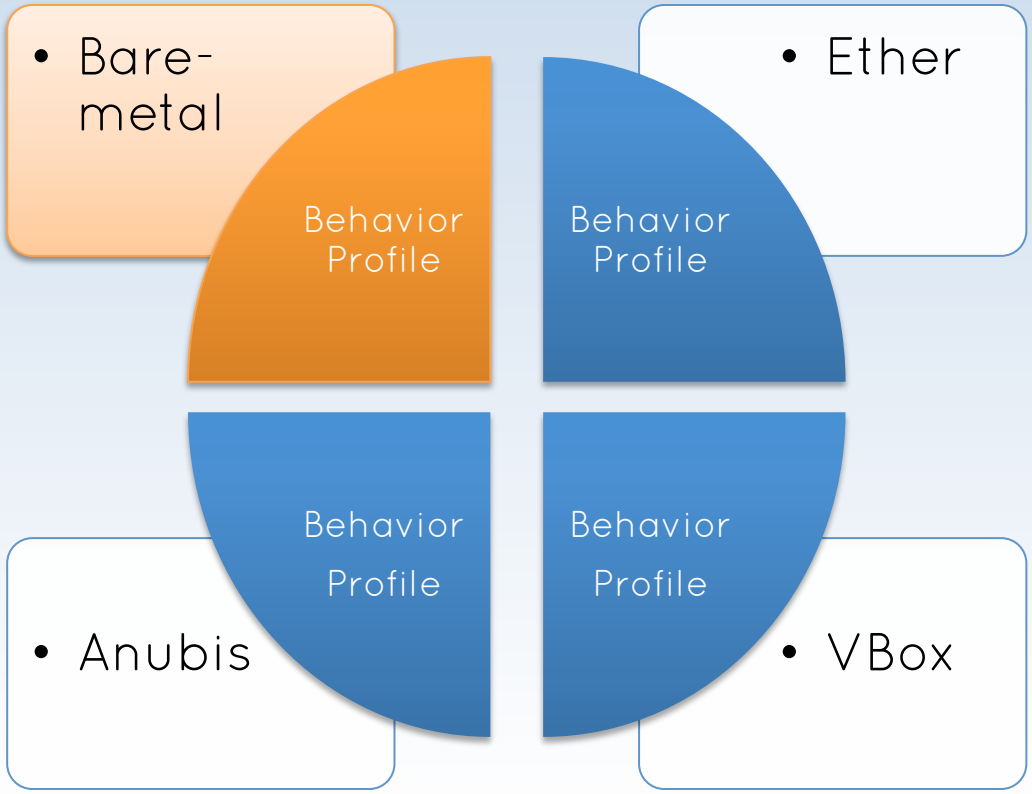
BareCloud



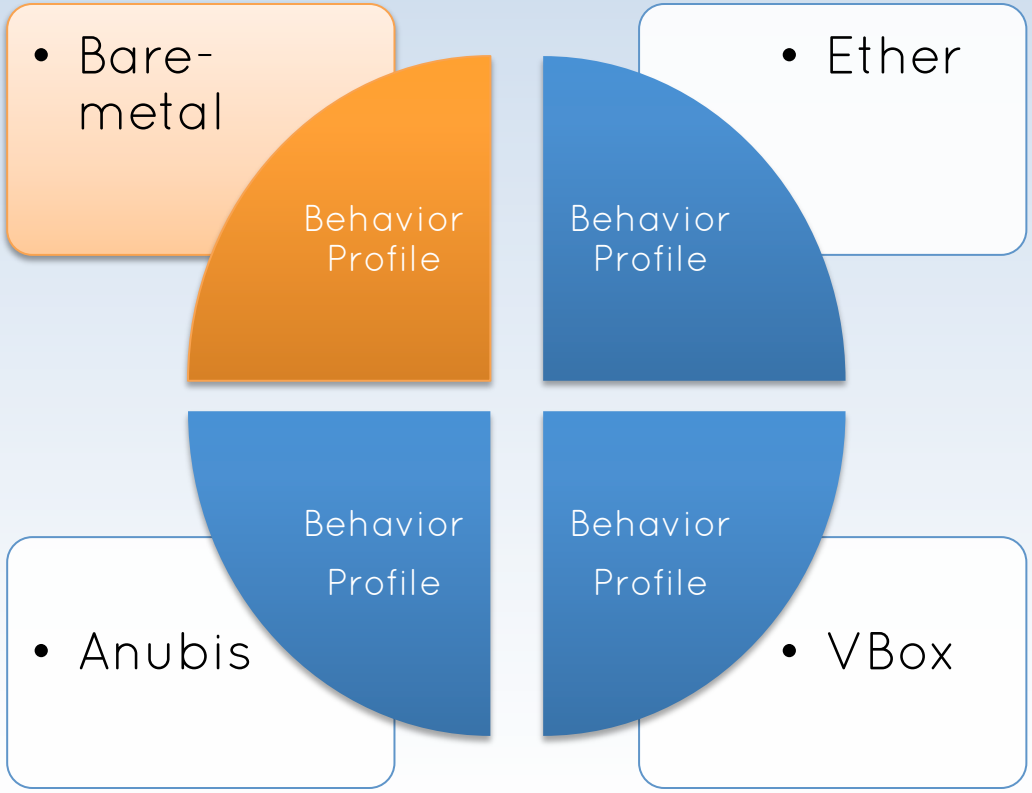
BareCloud


• Bare-metal
• Ether
Behavior Profile
Behavior Profile
Behavior Profile
• Anubis

BareCloud


• Bare-metal
Behavior Profile
• Ether
Behavior Profile
Behavior Profile
• Anubis
Behavior Profile
• VBox

BareCloud

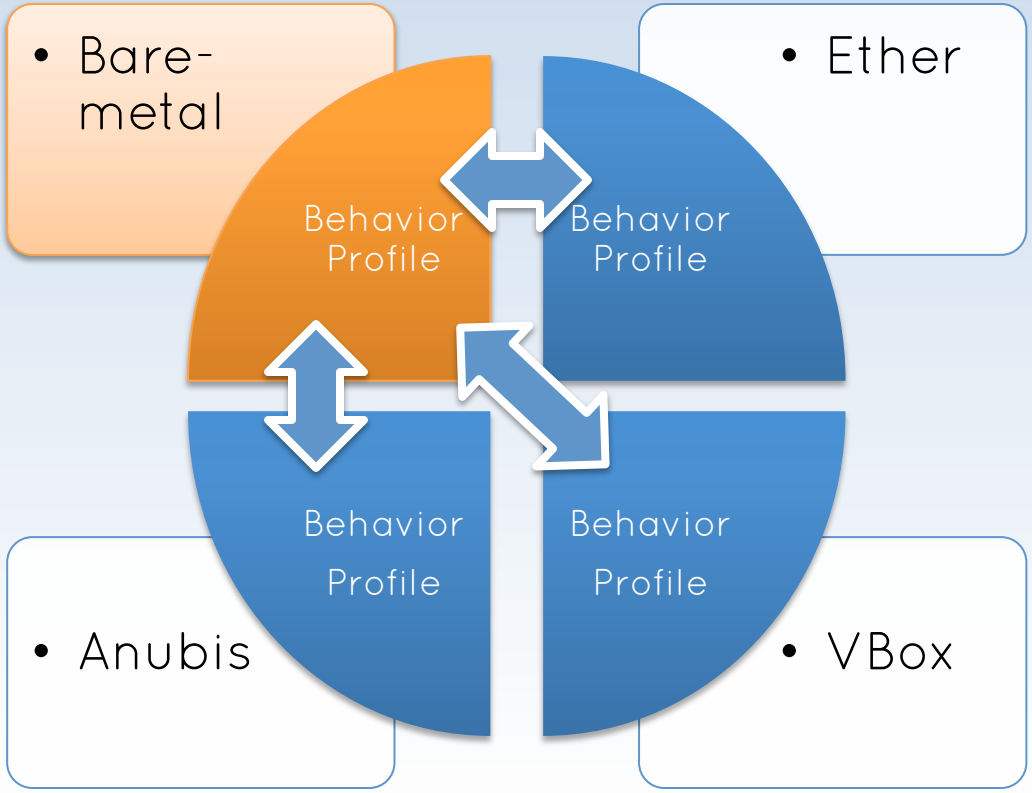

• Bare-metal
• Ether
Behavior Profile
Behavior Profile
Behavior Profile
Behavior Profile
• Anubis
• VBox


Xen™


QEMU
open source processor emulator

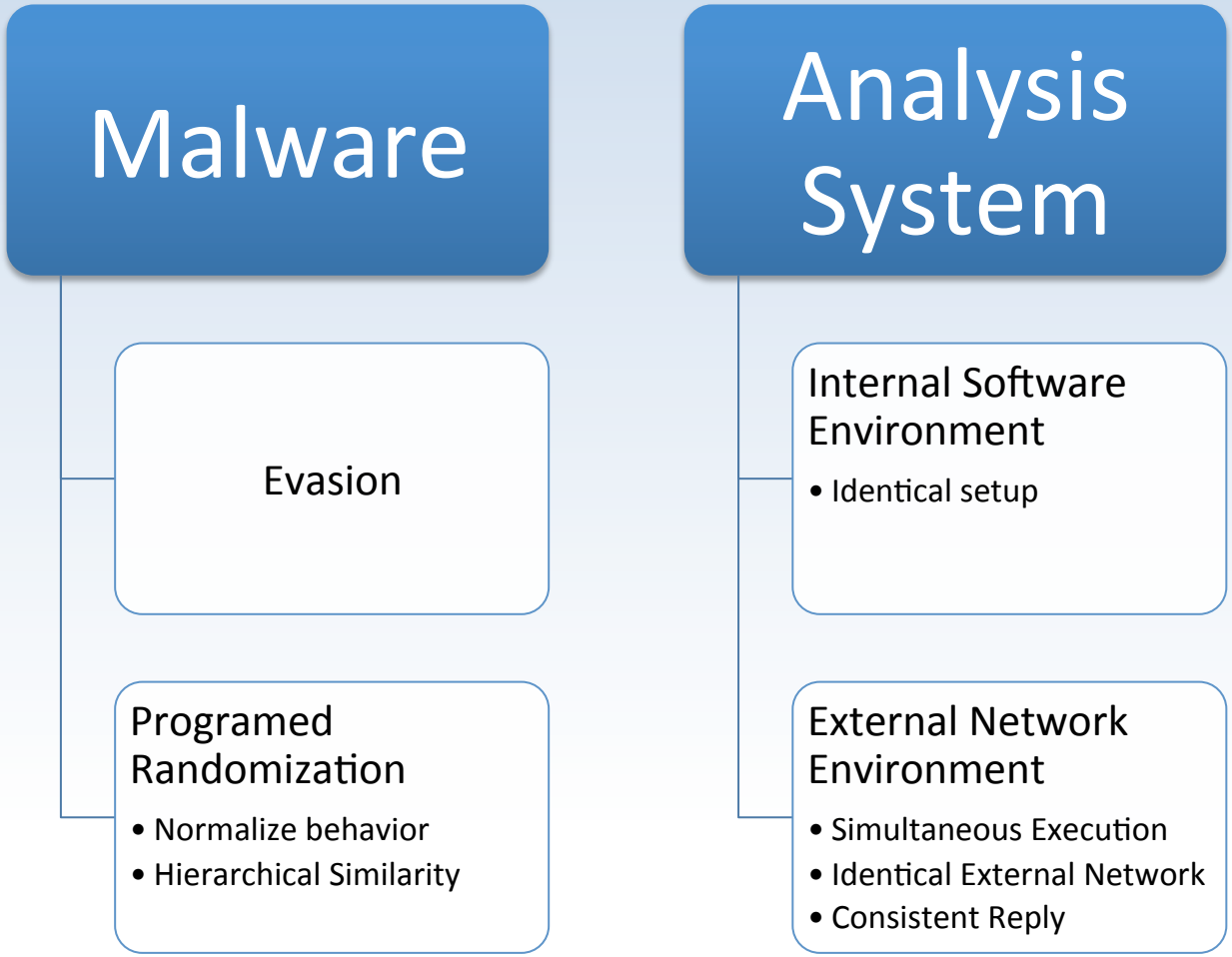

ORACLE
VirtualBox

BareCloud

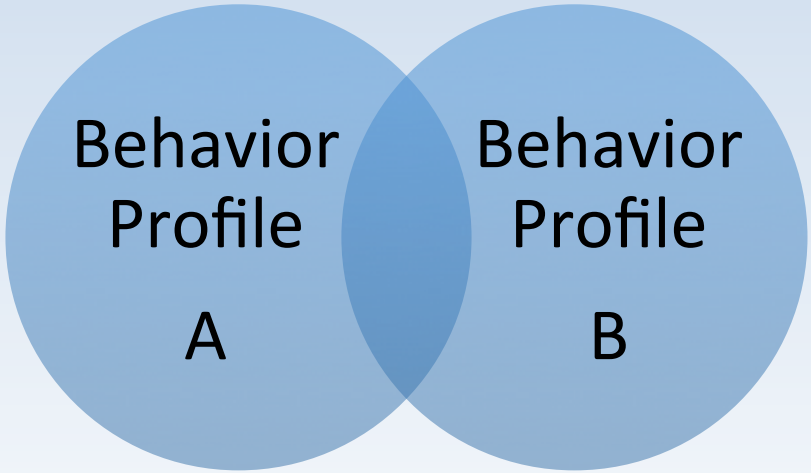

• Bare-metal
• Ether
Behavior Profile
Behavior Profile
Behavior Profile
Behavior Profile
• Anubis
• VBox

Transient vs. Persistent

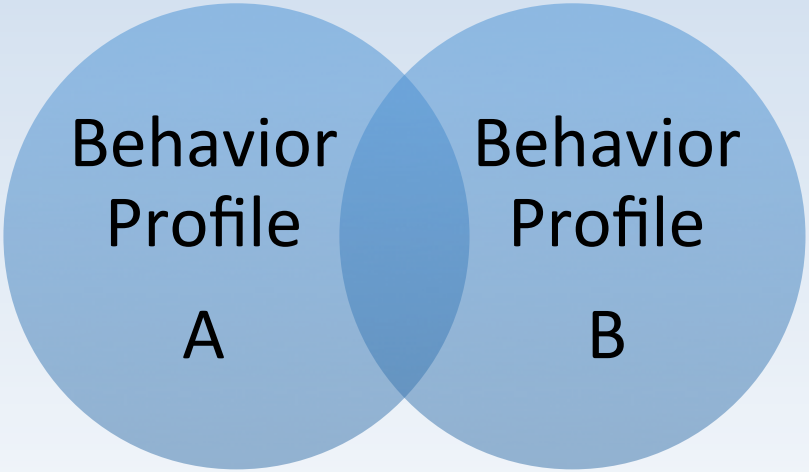
Behavior Deviation



Behavior Comparison

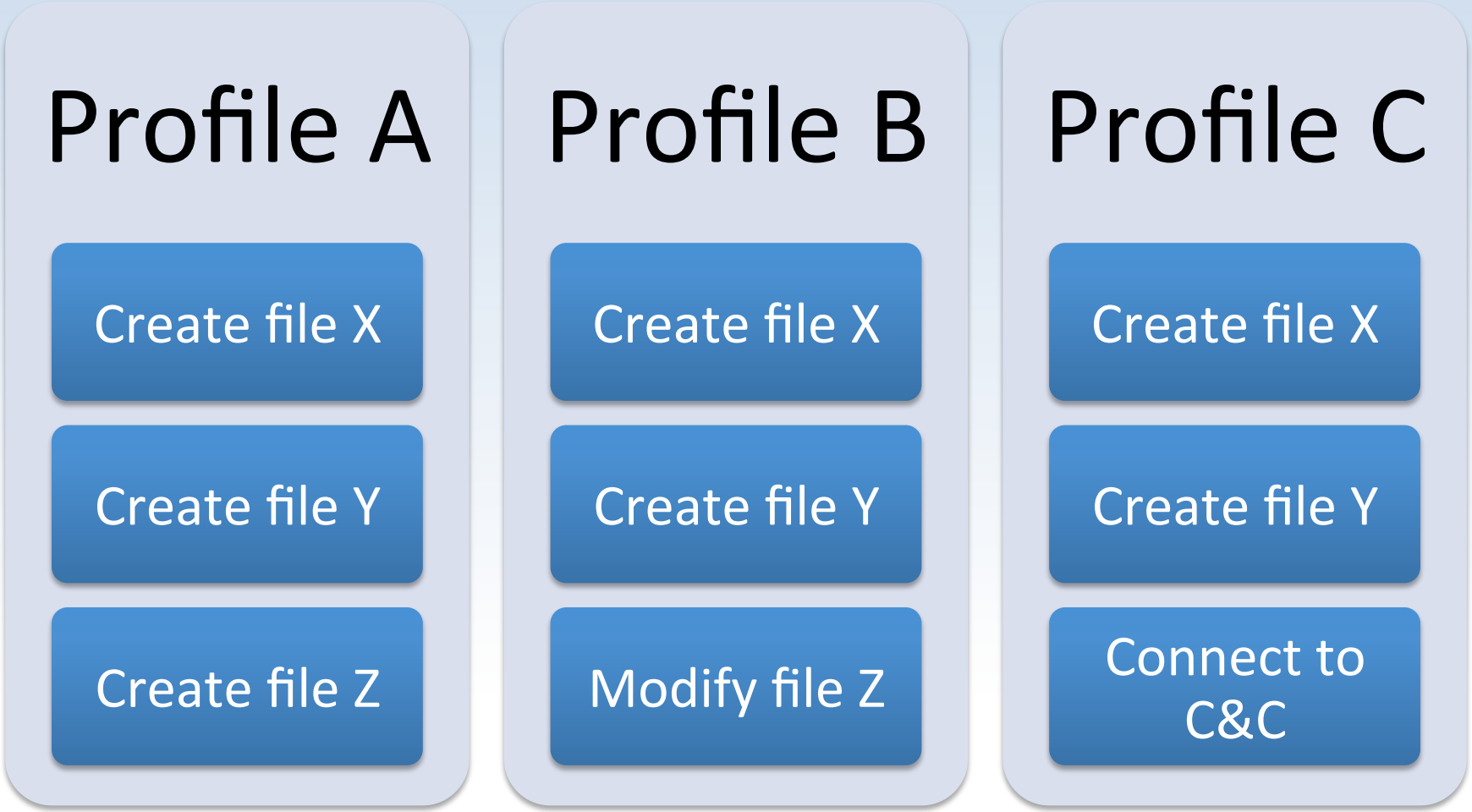


Behavior Comparison

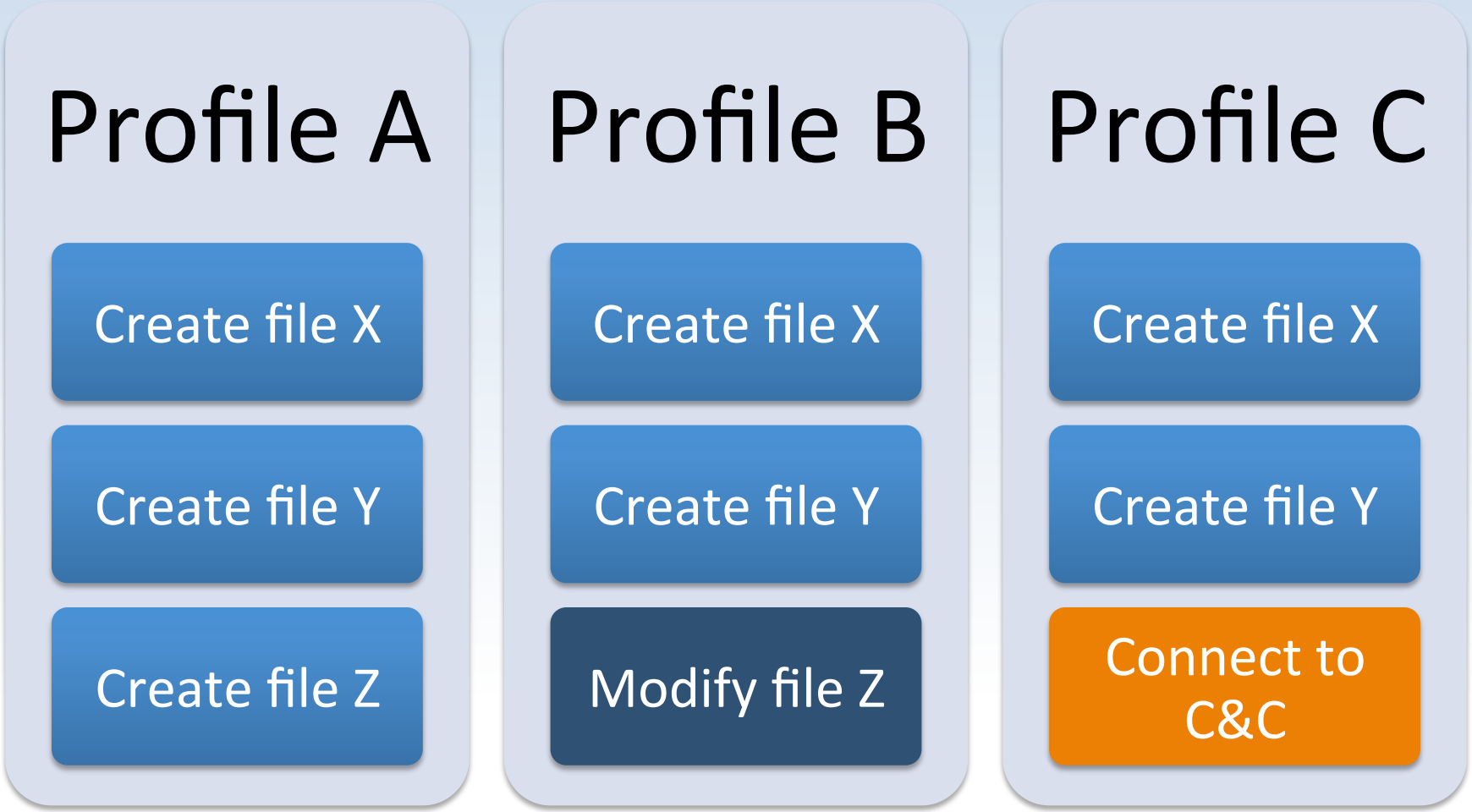


$$JaccardSimilarity = \frac{A \cap B}{A \cup B}$$

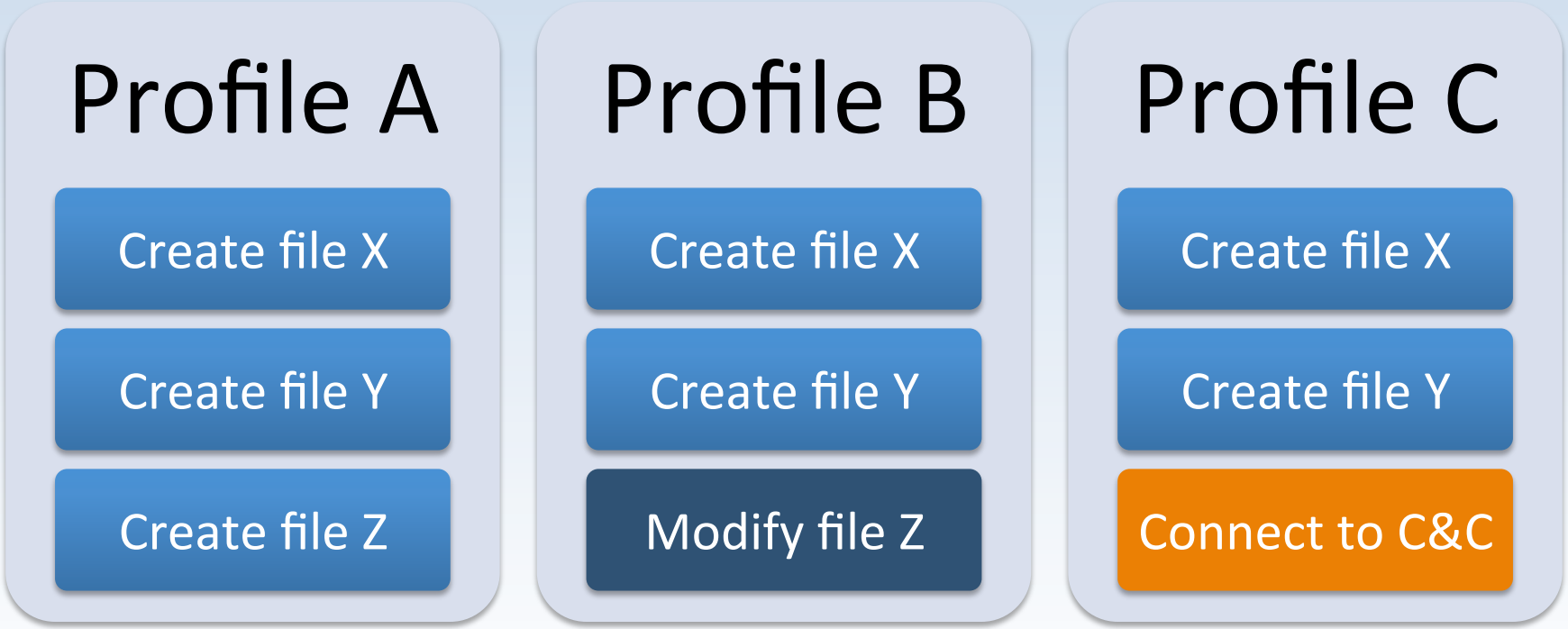
Behavior Comparison



Behavior Comparison

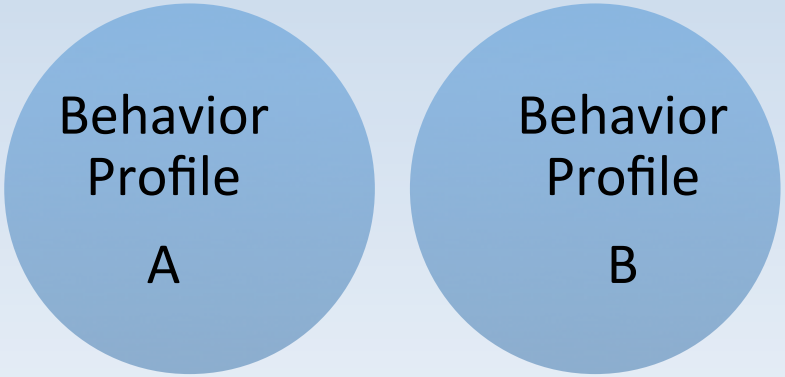


Behavior Comparison

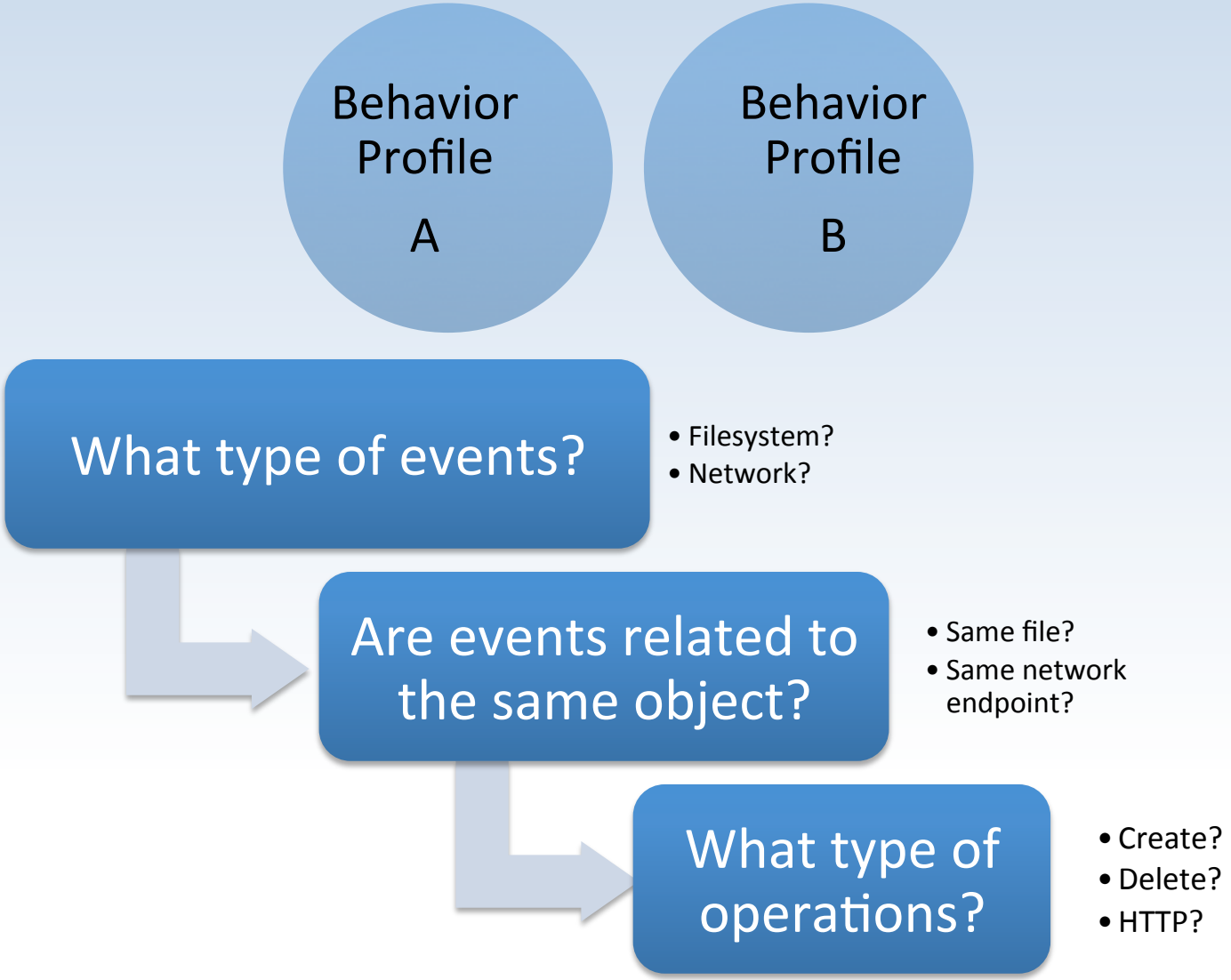


$$JaccardSimilarity(A, B) = 2/4 = JaccardSimilarity(A, C)$$

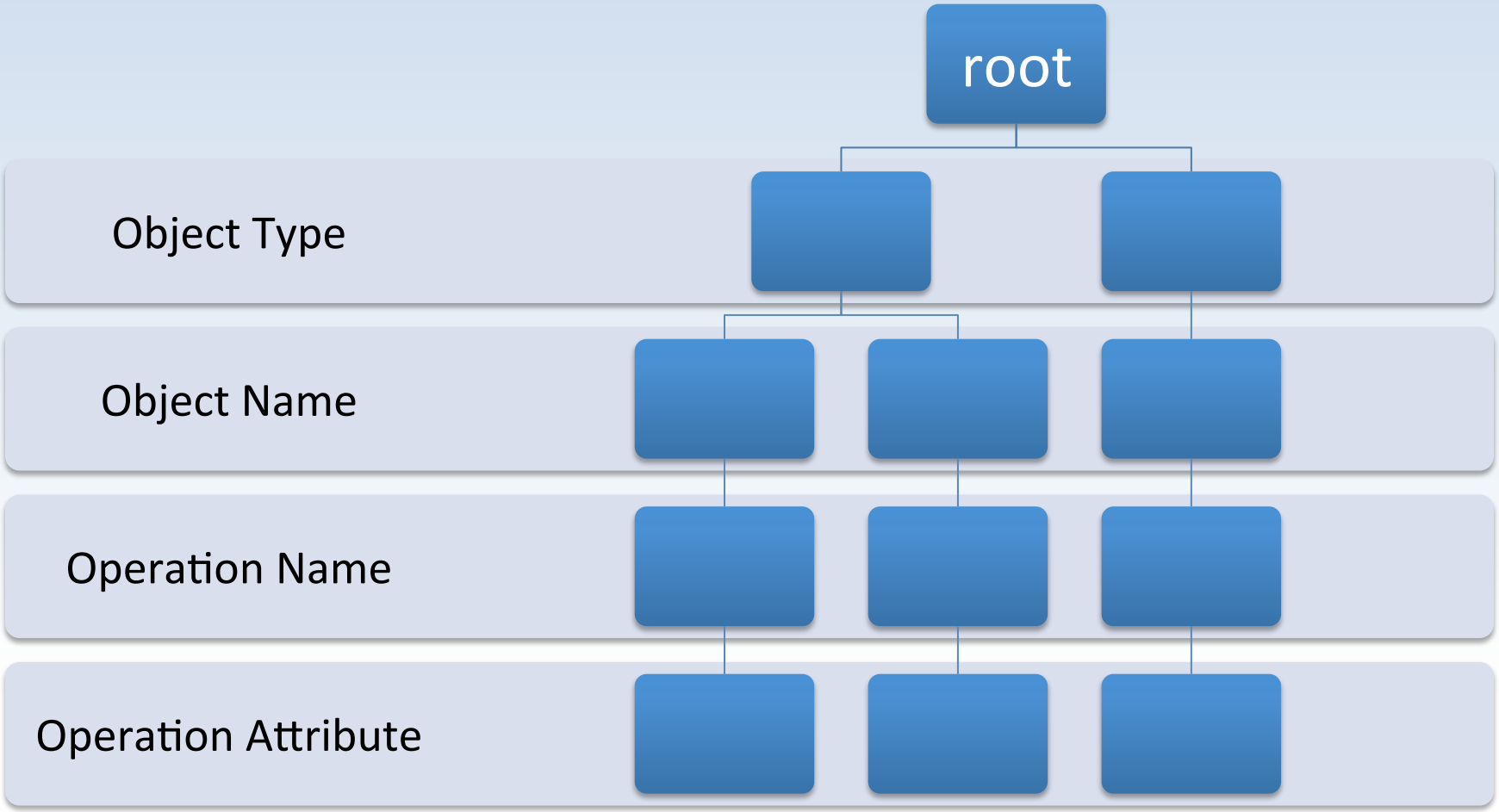
Behavior Comparison



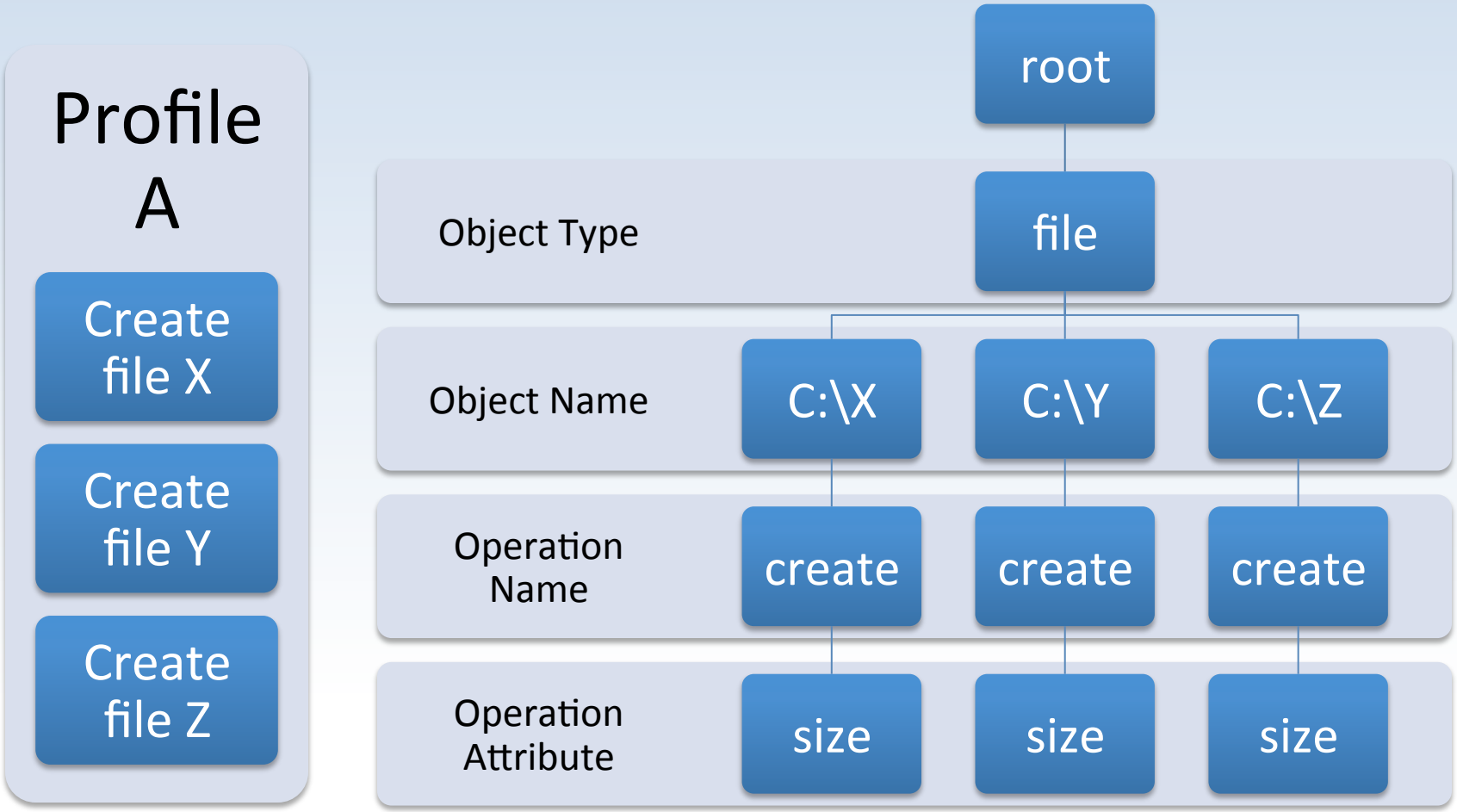
Behavior Comparison



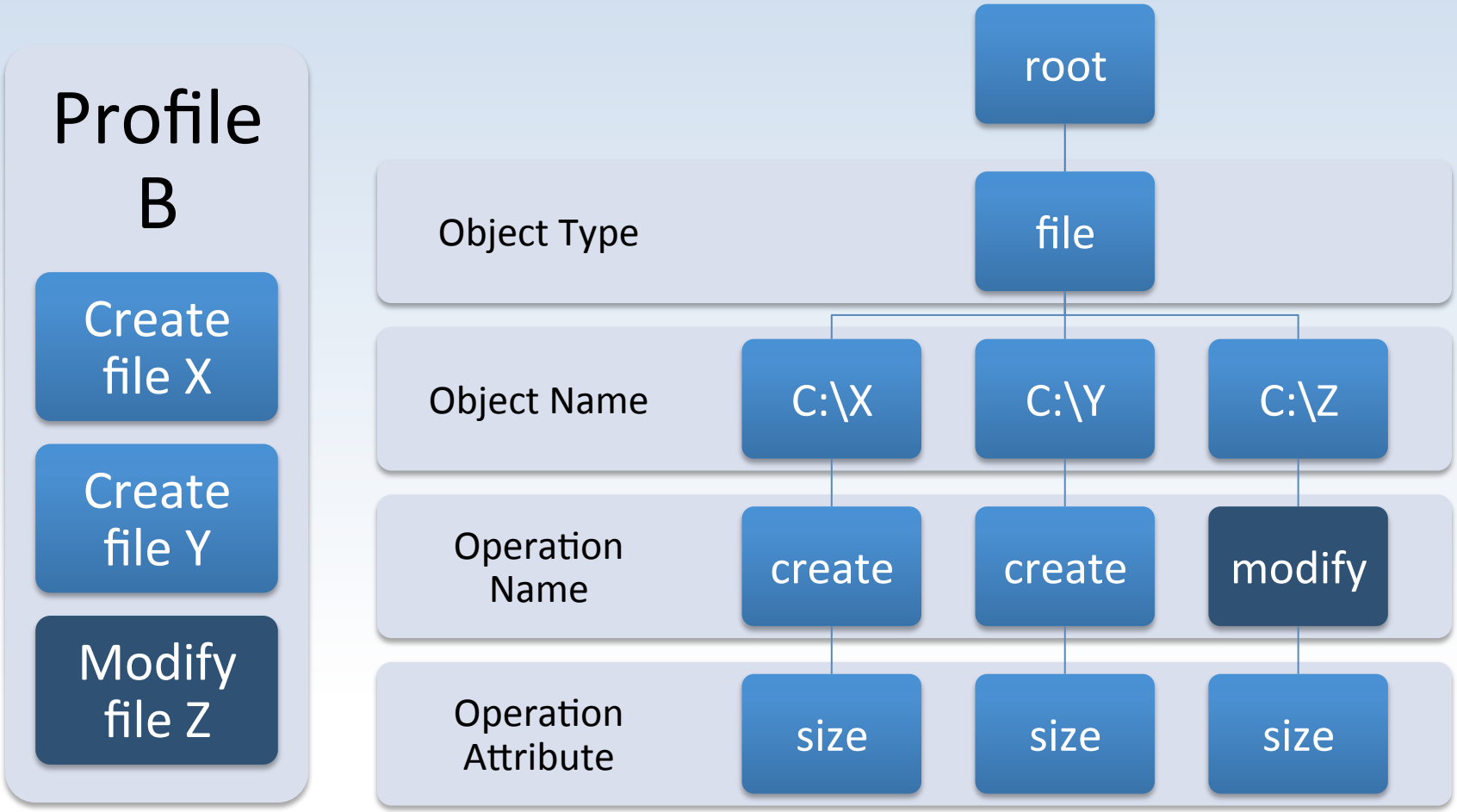
Behavior Similarity Hierarchy



Behavior Similarity Hierarchy



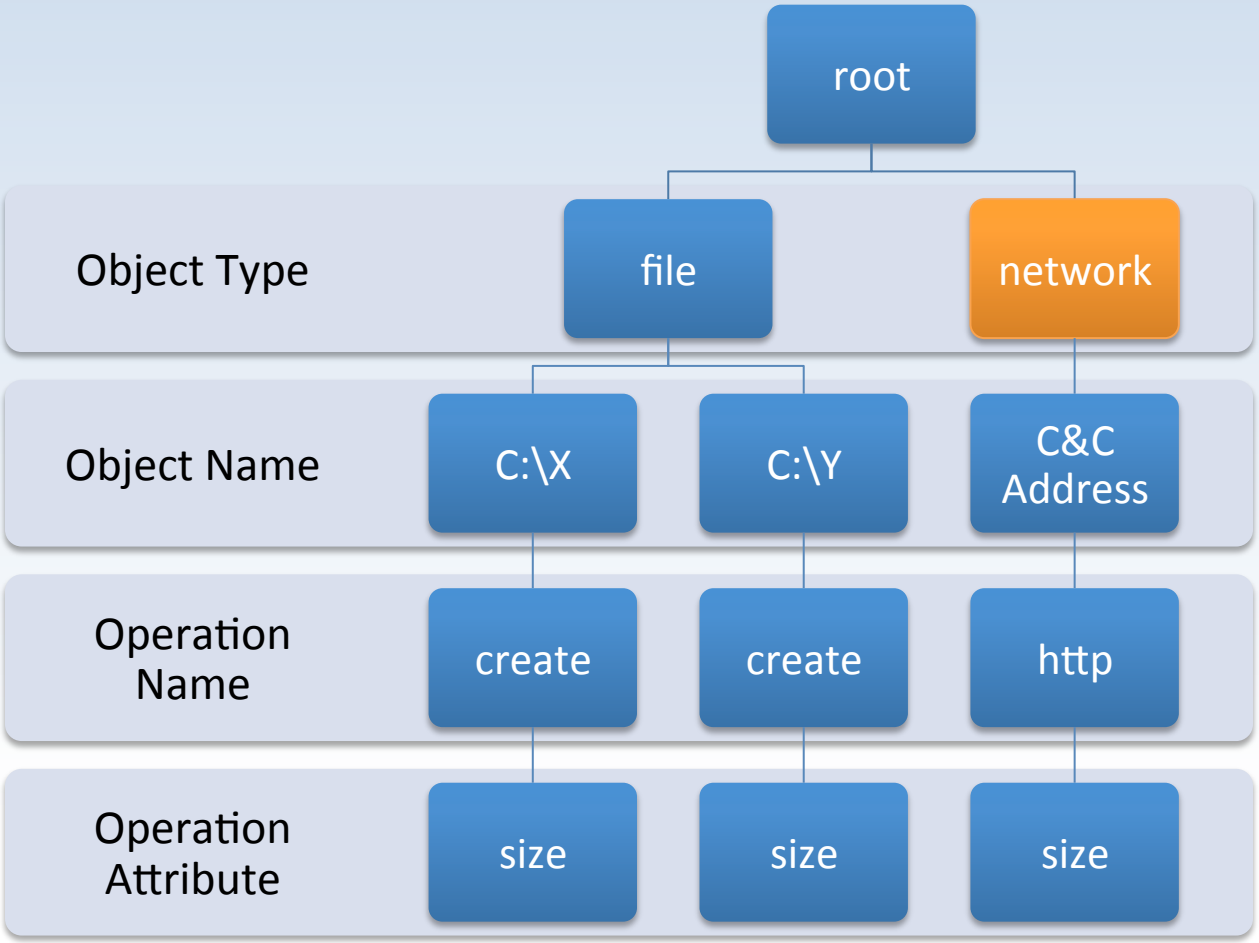
Behavior Similarity Hierarchy



Behavior Similarity Hierarchy

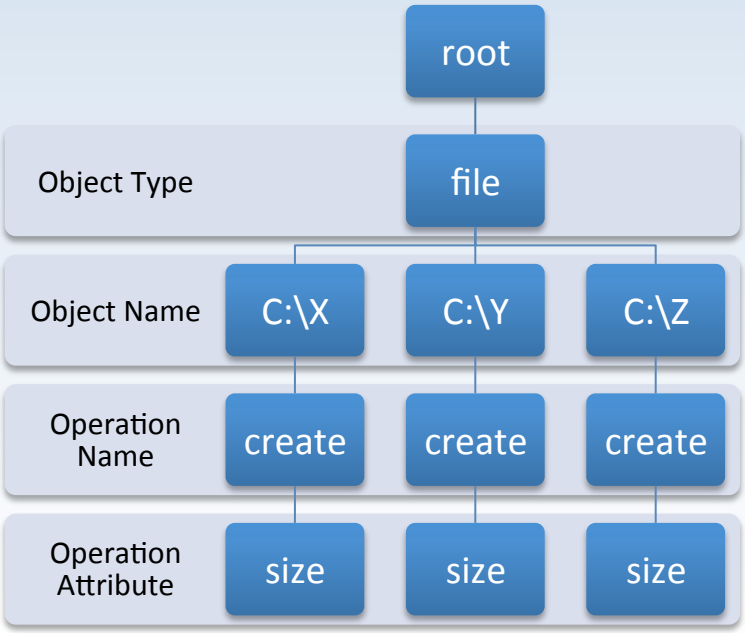
Profile C

- Create file X
- Create file Y
- Connect to C&C

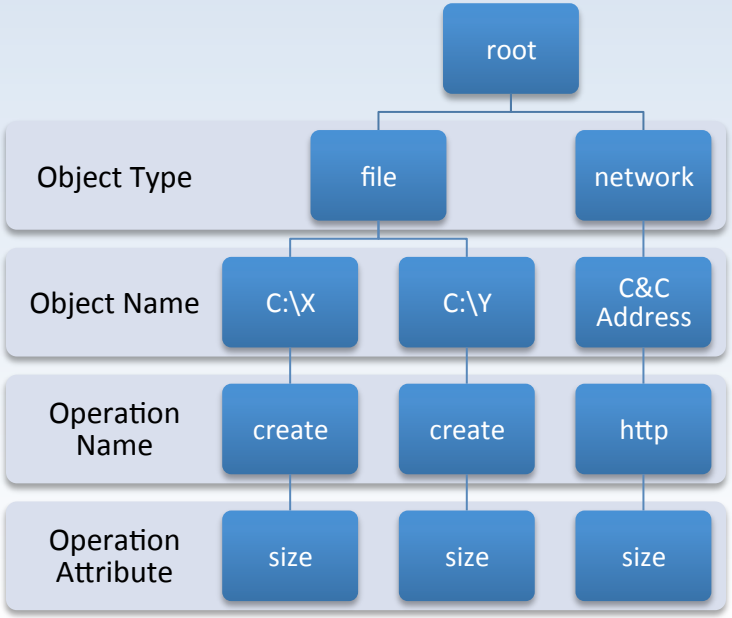


Hierarchical Similarity

Profile A



Profile C

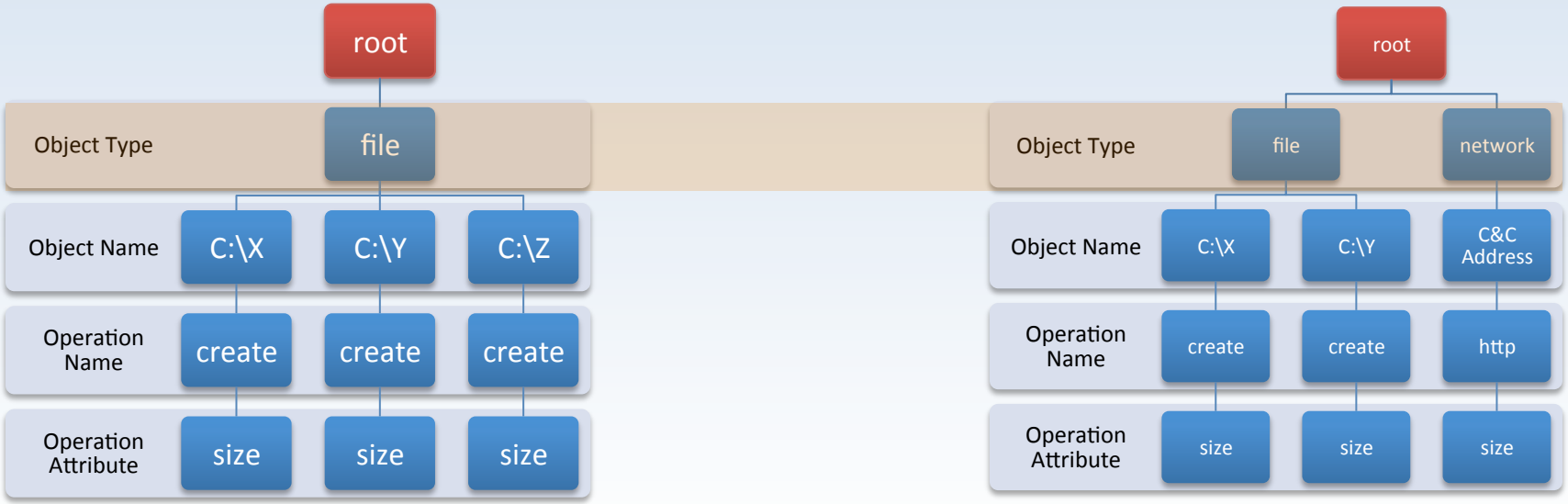


Hierarchical Similarity

Profile A

Profile C

Candidate Sets



Hierarchical Similarity

Profile A

Profile C

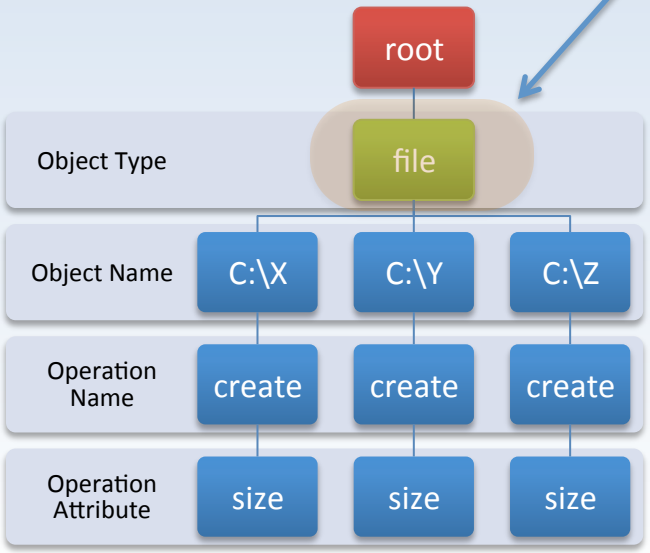
Candidate Sets

Hierarchical Similarity

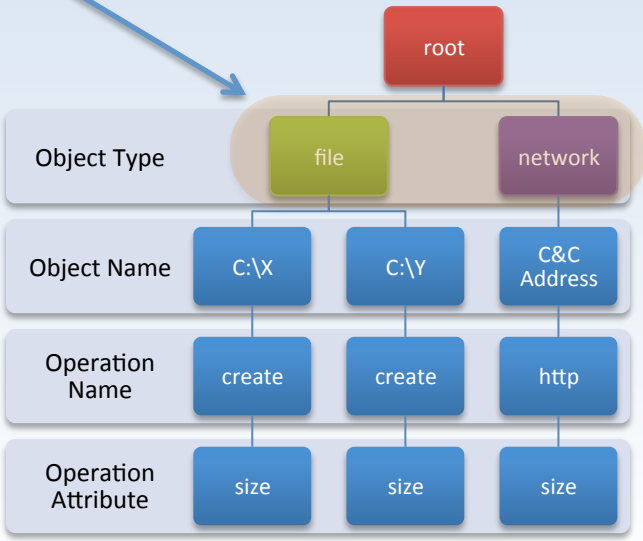
Profile A

Profile C

Candidate Sets



$Sim_1 = 1/2$

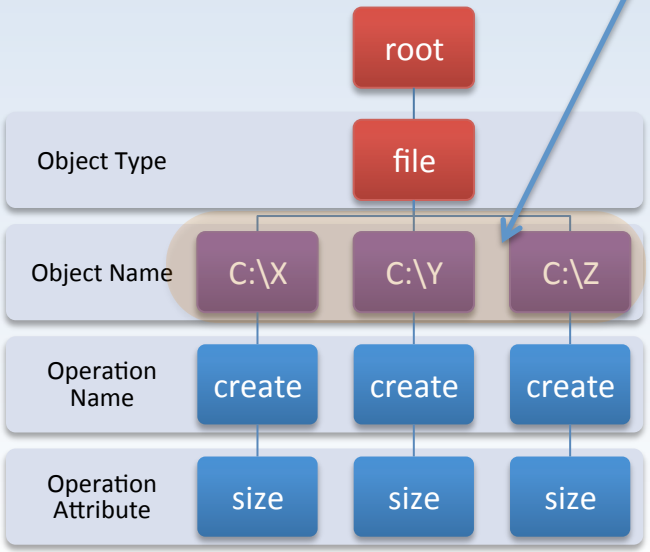


Hierarchical Similarity

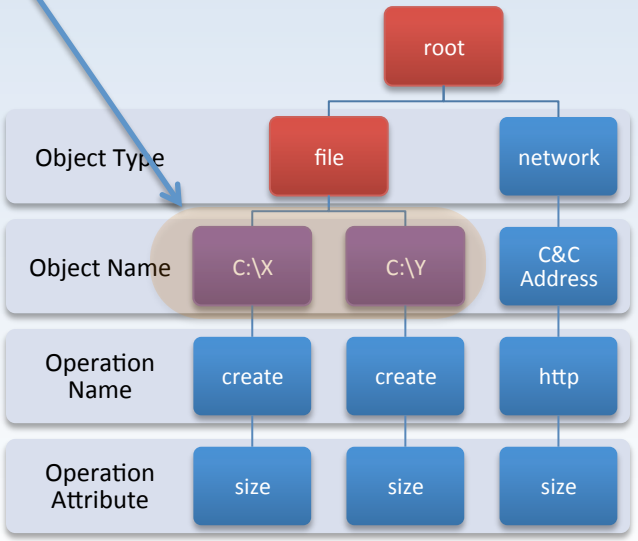
Profile A

Profile C

Candidate Sets

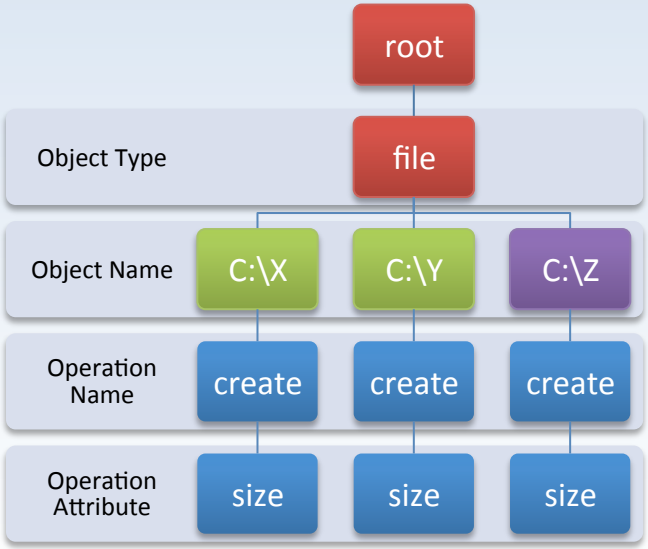


$Sim_1 = 1/2$



Hierarchical Similarity

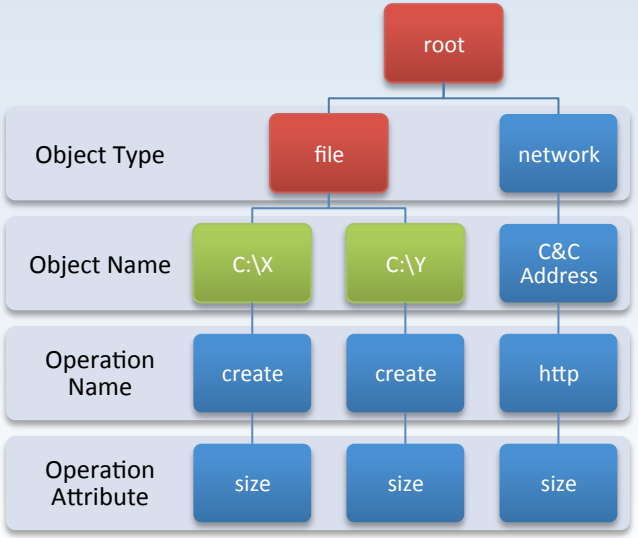
Profile A



$Sim_1 = 1/2$

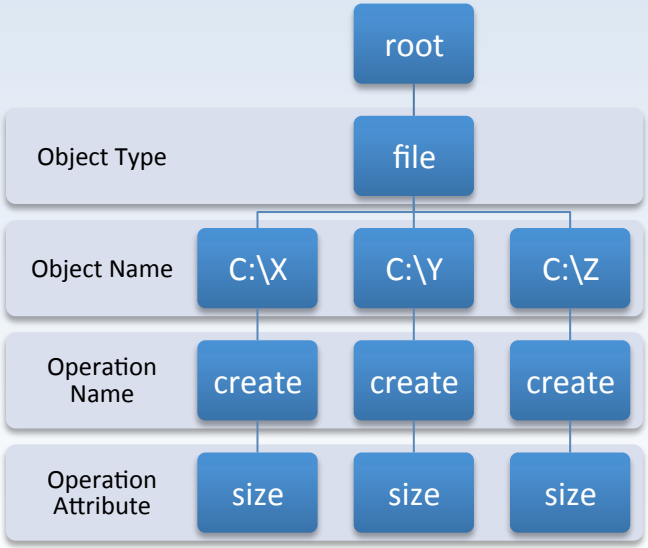
$Sim_2 = 2/3$

Profile C



Hierarchical Similarity

Profile A



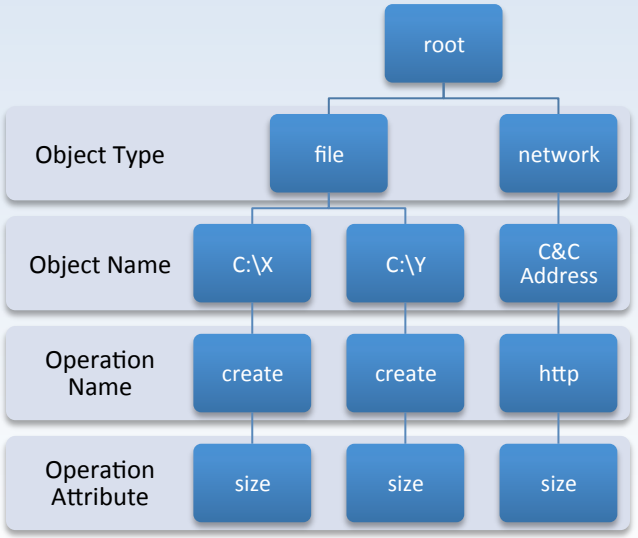
$Sim_1 = 1/2$

$Sim_2 = 2/3$

$Sim_3 = 1$

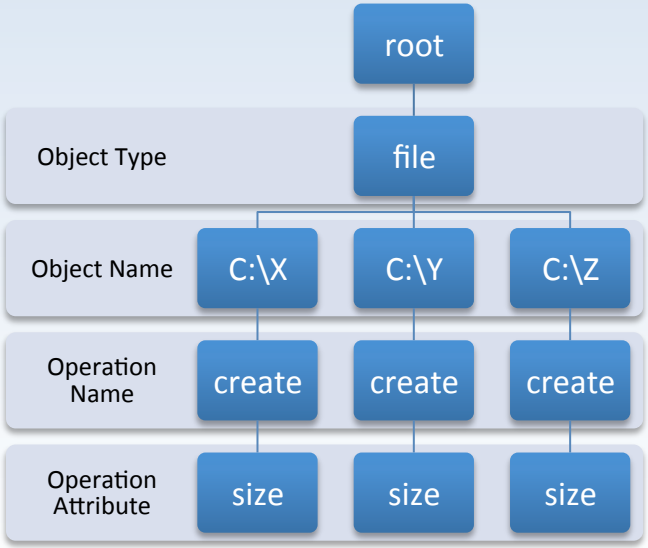
$Sim_4 = 1$

Profile C



Hierarchical Similarity

Profile A



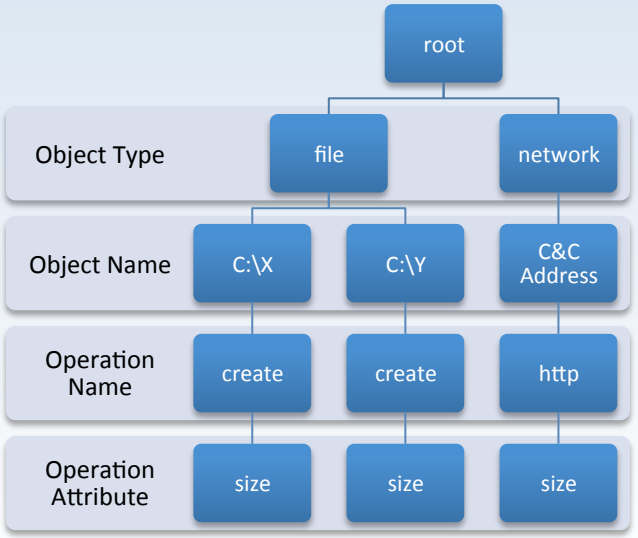
$Sim_1 = 1/2$

$Sim_2 = 2/3$

$Sim_3 = 1$

$Sim_4 = 1$

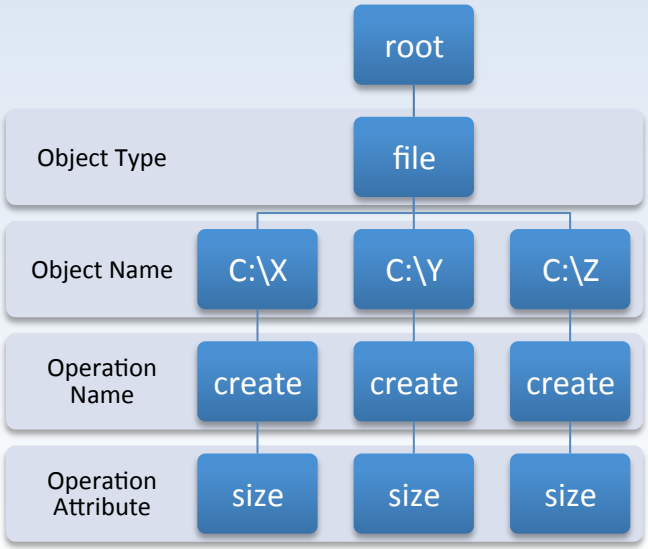
Profile C



$$Sim(A, C) = AVG(Sim_1 \ldots Sim_4) = 0.79$$

Hierarchical Similarity

Profile A



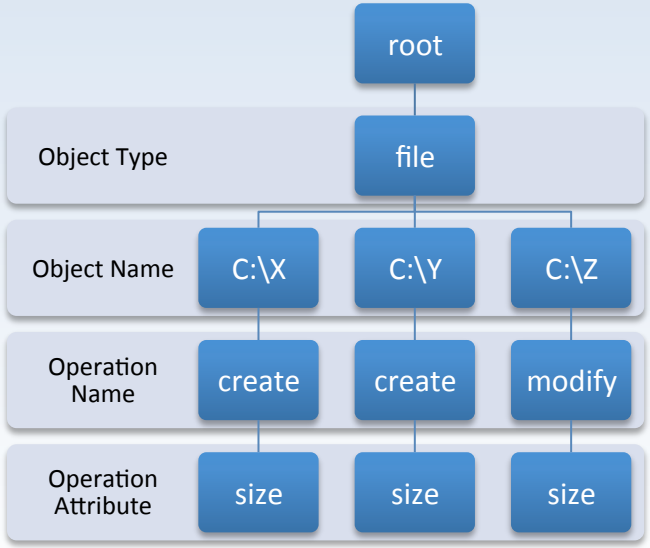
$Sim_1 = 1$

$Sim_2 = 1$

$Sim_3 = 1/2$

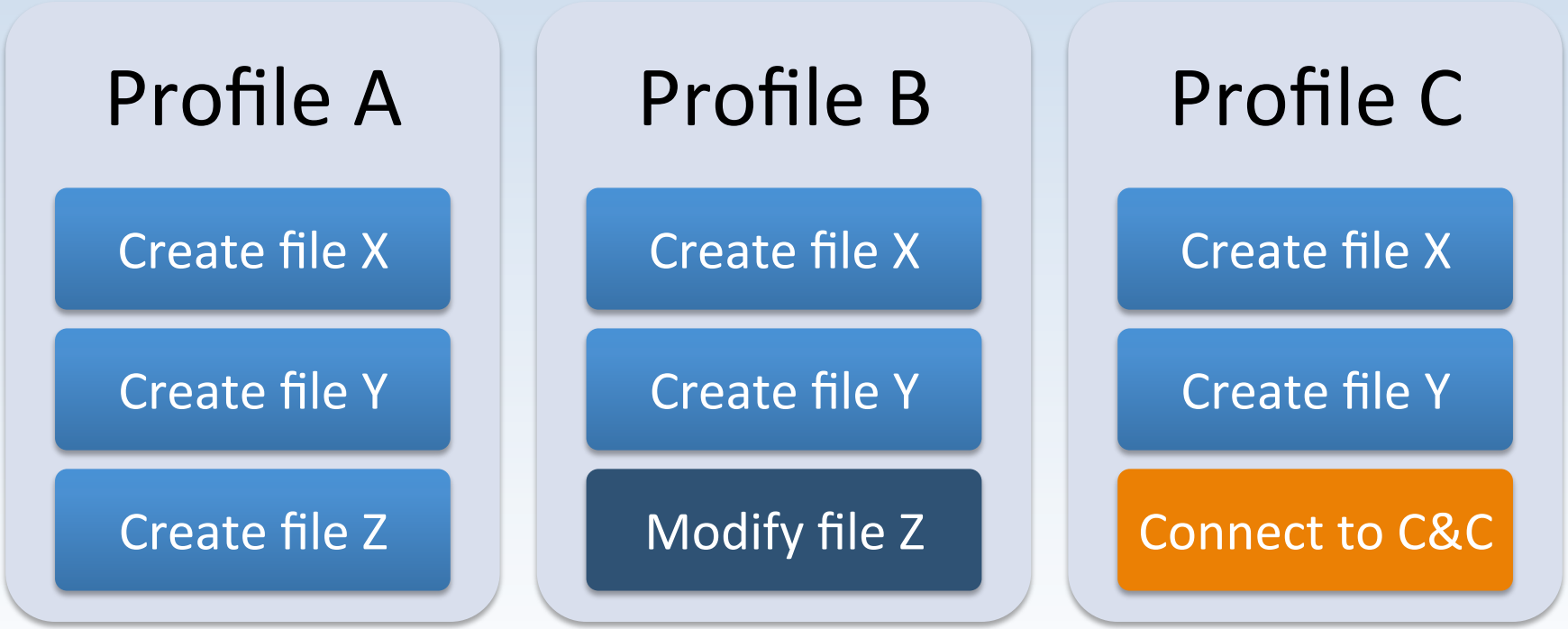
$Sim_4 = 1$

Profile B



$$Sim(A, B) = AVG(Sim_1 \ldots Sim_4) = 0.87$$

Behavior Comparison



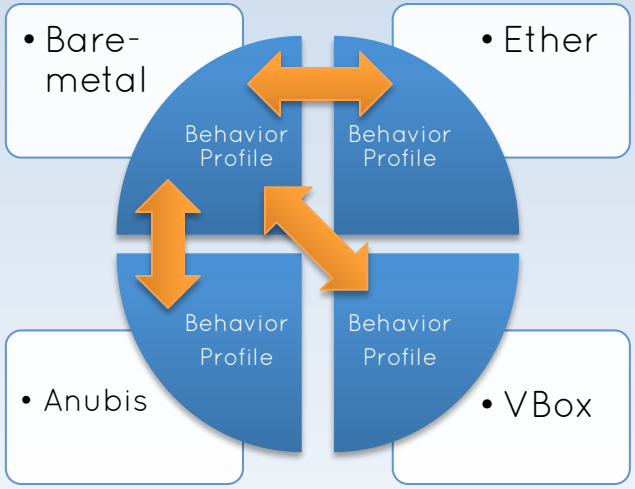
$$JaccardSimilarity(A, B) == JaccardSimilarity(A, C)$$

$$HierarchicalSim(A, B) > HierarchicalSim(A, C)$$
$$0.87 > 0.79$$

Deviation Score

- Behavior Distance

$$Distance(A, B) = 1 - Sim(A, B)$$



- Deviation Score D

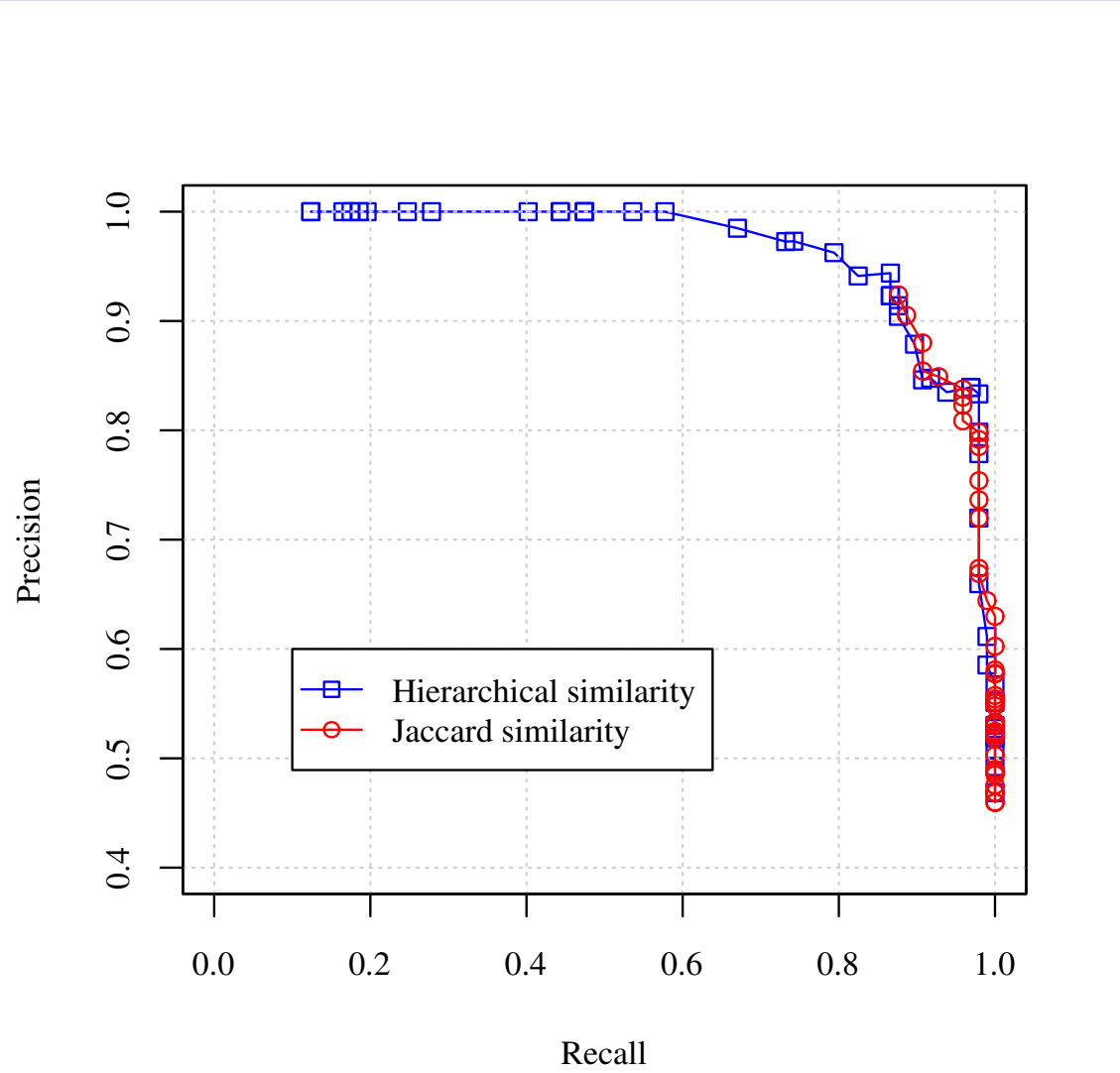
  Quadratic mean of the behavior distances with respect to the bare-metal analysis

- Deviation Threshold t
  - Evasive if $D > t$

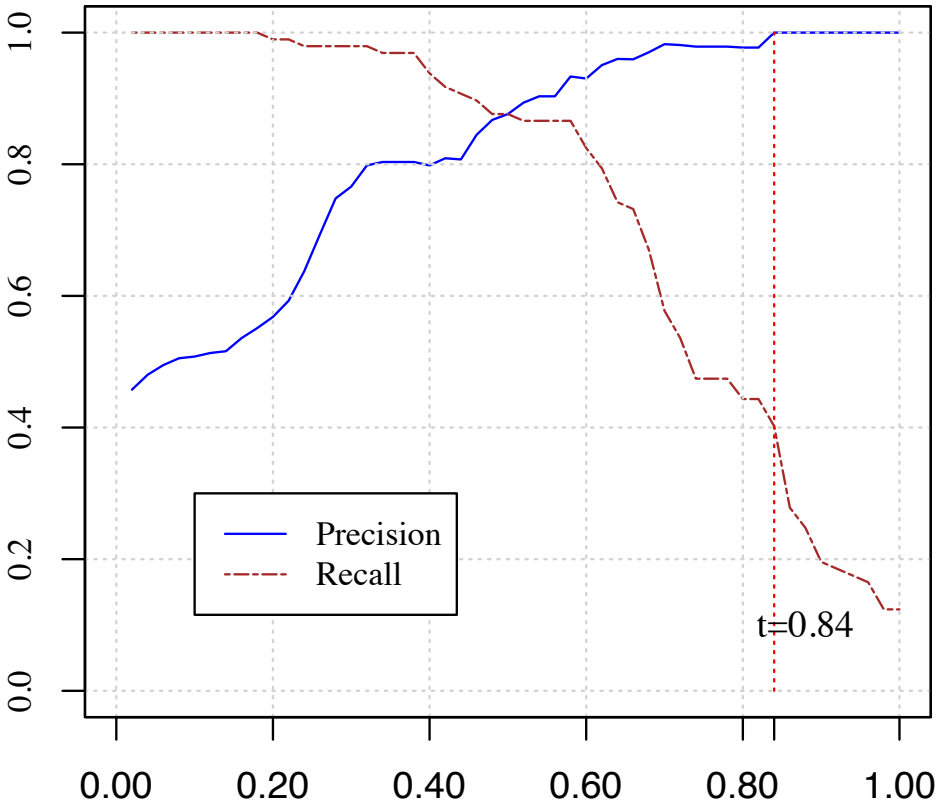
Evaluation

- Ground truth
  - 111 evasive samples (29 families)
  - 119 non-evasive samples (49 families)
- Calculated behavior Deviation score $\mathbf{D}$
- Calculate Jaccard distance-based deviation $\mathbf{JD}$
  - Maximum Jaccard-distance among different behavior profiles of a malware
- Precision-recall analysis by varying the deviation threshold $\mathbf{t}$

Evaluation


Precision
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.0
0.2
0.4
0.6
0.8
1.0
Recall
Hierarchical similarity
Jaccard similarity

Evaluation


1.0
0.8
0.6
0.4
0.2
0.0
0.00
0.20
0.40
0.60
0.80
1.00
Precision
Recall
t=0.84
Threshold (t)

Large-scale Evaluation

- Recent real-world malware feed observed by Anubis
- Randomly select samples with
  - low system and low network activity
  - high system and high network activity
  - high system but low network activity
  - Low system but high network activity
- 110,005 samples
  - 4 months period beginning from July 2013

Large-scale Evaluation

Environment	Detection Count	Percentage
Anubis	4947	84.78
Ether	4562	78.18
VirtualBox	3576	61.28
All	2530	43.35

5,835 evasive malware out of 110,005 recent samples

Limitations

- Hardware vs software iSCSI initiator
- Stalling code
  - Wait for user input
  - Advanced waiting
- Decoy reconnaissance
  - Real hardware ID not randomized

Conclusions

- Evasive Malware is a real threat to the new wave of dynamic analysis based malware detection systems
- We presented a system that can detect these evasive malware automatically

Thank You!

Questions