The understandability challenge in building diagnostic systems for ~~non-experts~~ everyone but the omniscient admin

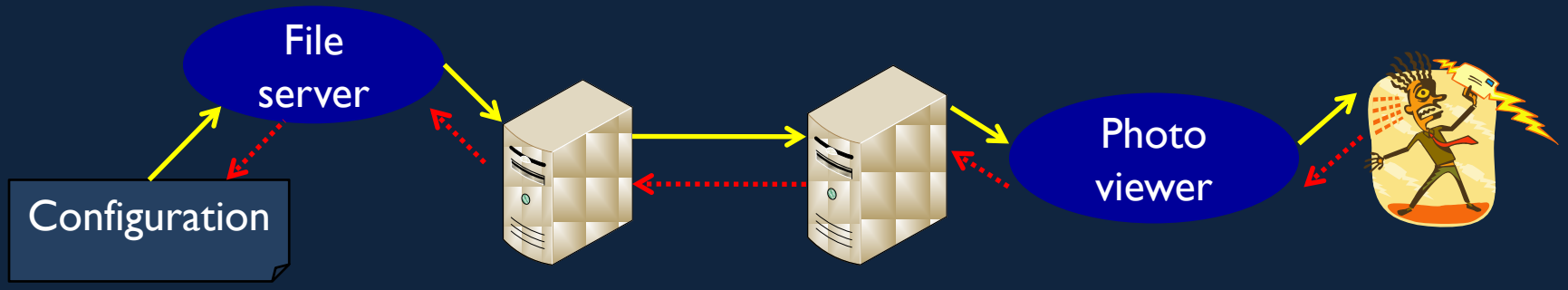
Ratul Mahajan
Microsoft Research

UW MSR summer institute 2009

Diagnosis explains faulty behavior

Starts with problem symptoms

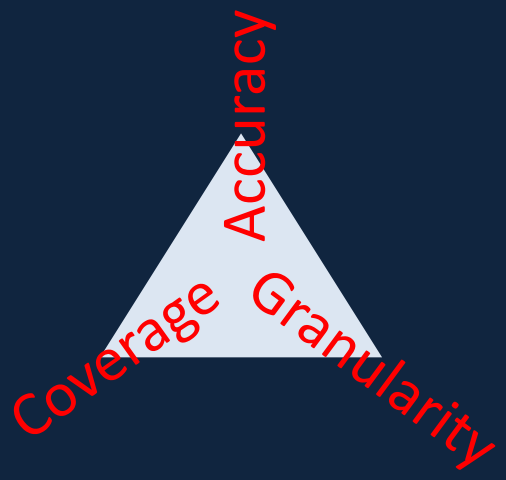
Ends at likely cause(s)

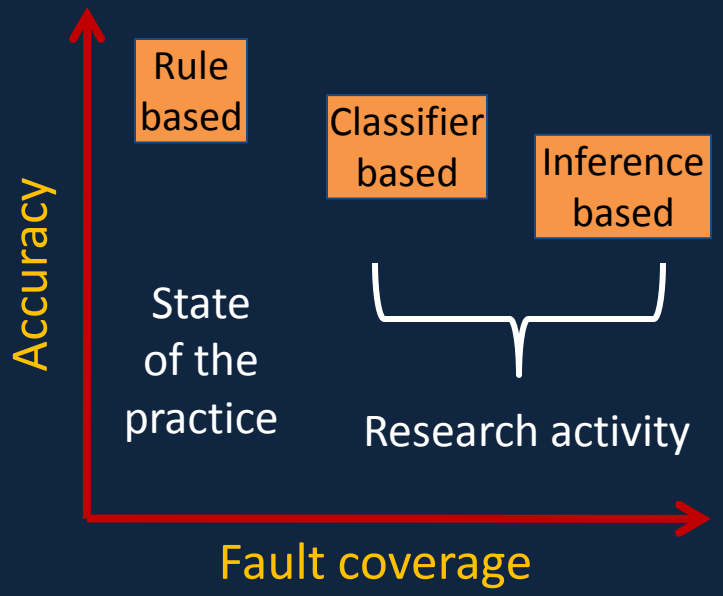


Configuration change denies permission

User cannot access a remote folder

Common considerations for a diagnostic system





Accuracy: How often the real culprit is identified

Coverage: Fraction of failures covered

Granularity: The detail at which culprit are identified

NetMedic: A detailed diagnostic system

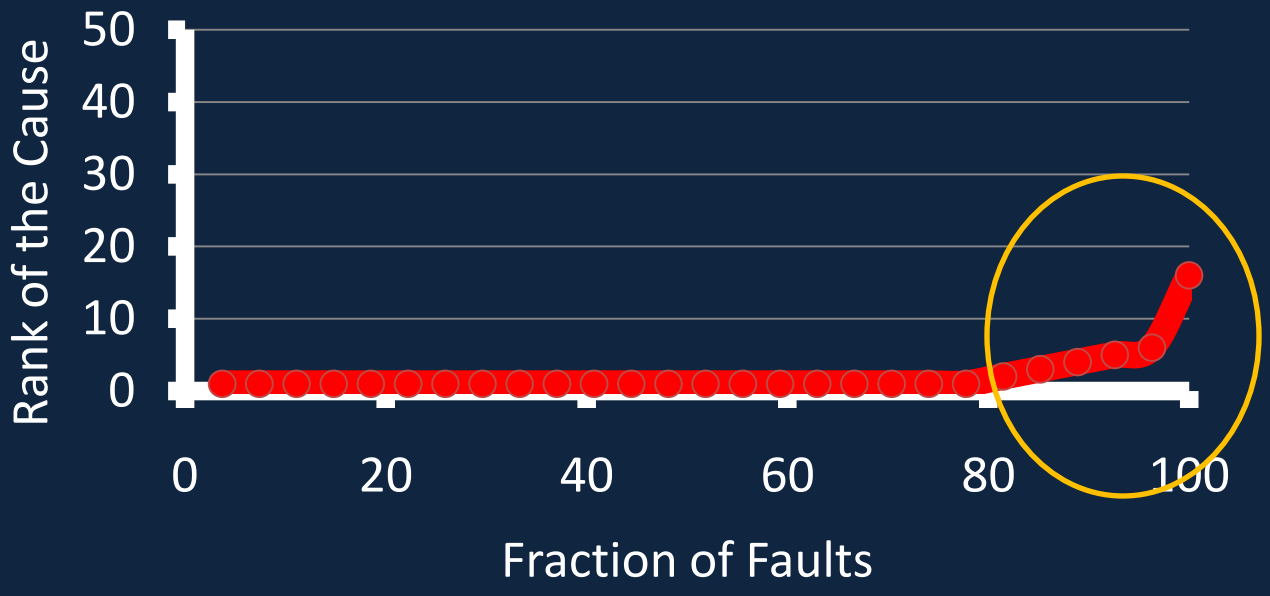
Focus on small enterprises as a starting point

Inference based:

- Views the network as a dependency graph of fine-grained components (e.g., applications, services)
- Produces a ranked list of likely culprit components using statistical and learning techniques

[Detailed diagnosis in enterprise networks, SIGCOMM 2009]

Effectiveness of NetMedic



Identifies the real culprit as the most likely 80% of the time but not always

Unleashing NetMedic-like systems on users

Understandability became a key hurdle

- How to present the analysis to the user?
- Impacts mean time to recovery

Two sub-problems at the intersection of systems and HCI

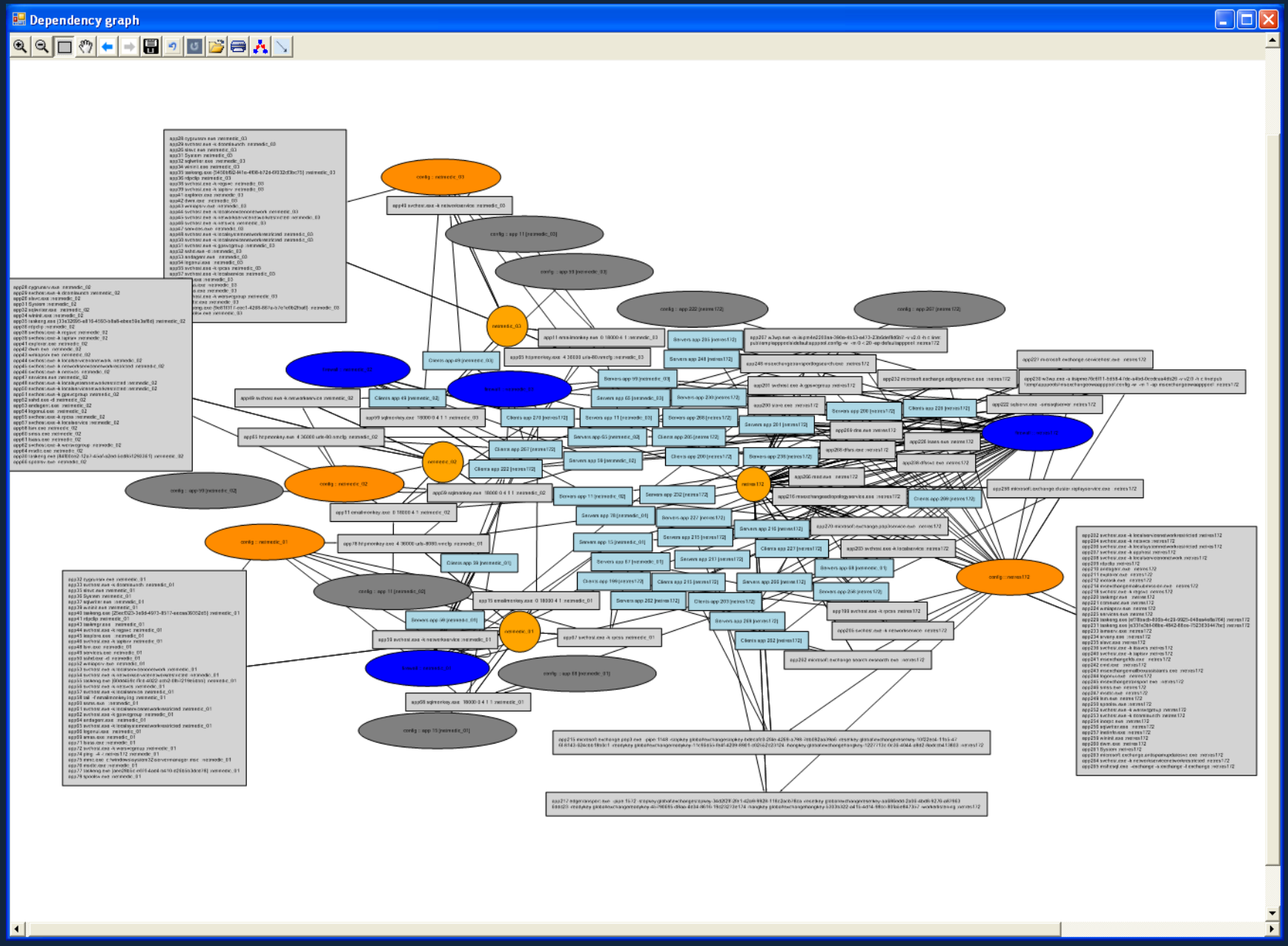
- Uncertainty visualization
- Intuitiveness of analysis

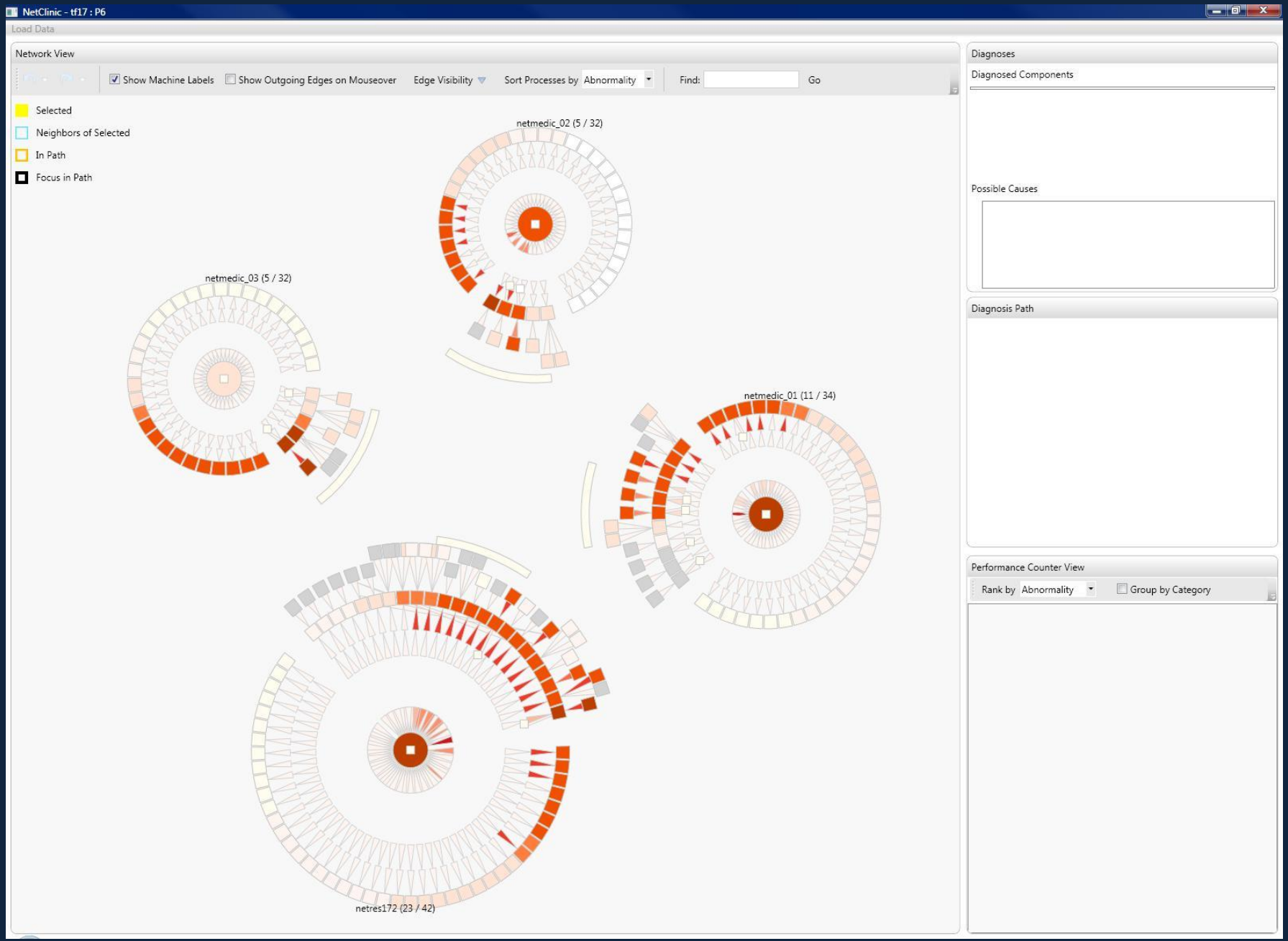
Uncertainty visualization

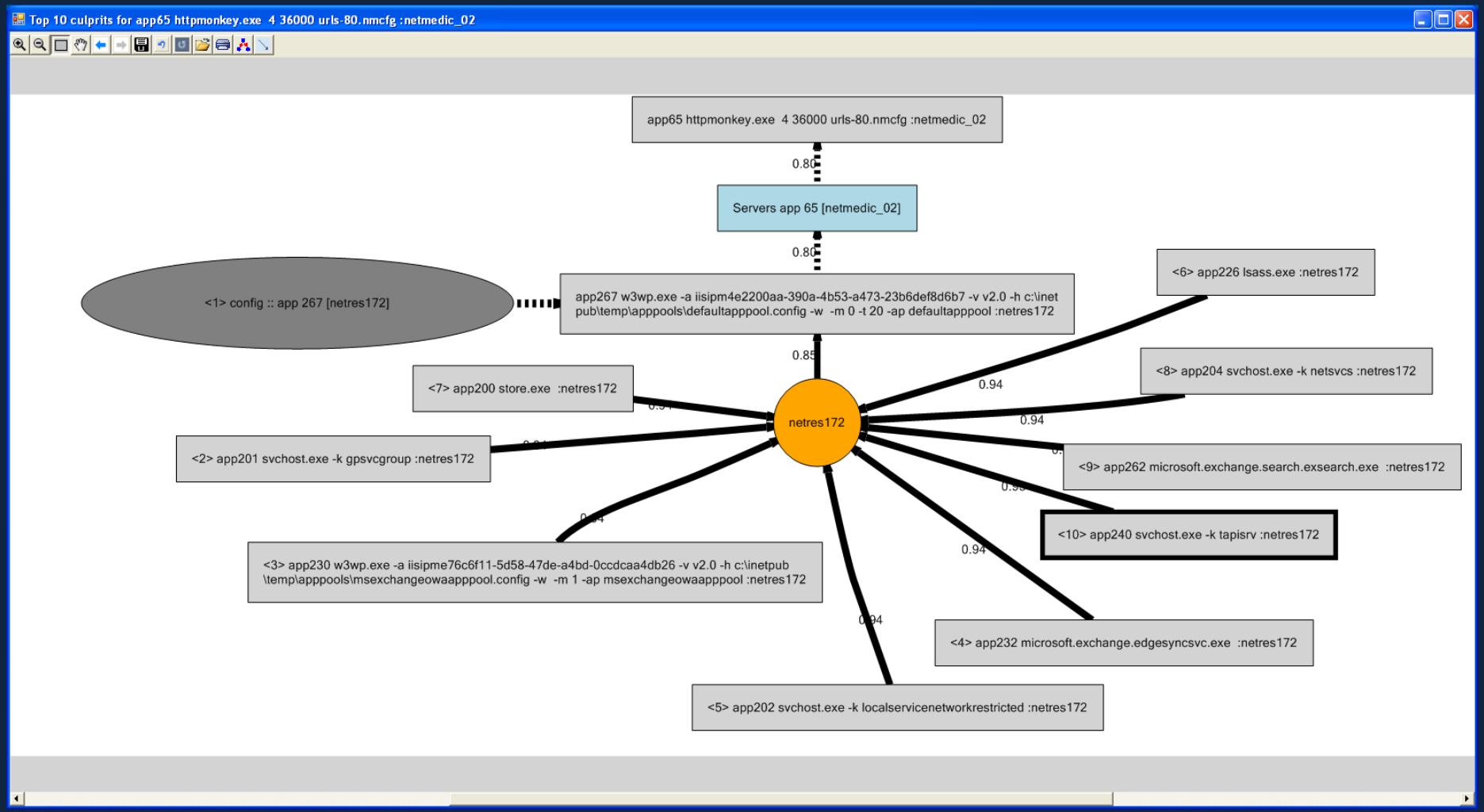
Presenting the results of statistical analysis

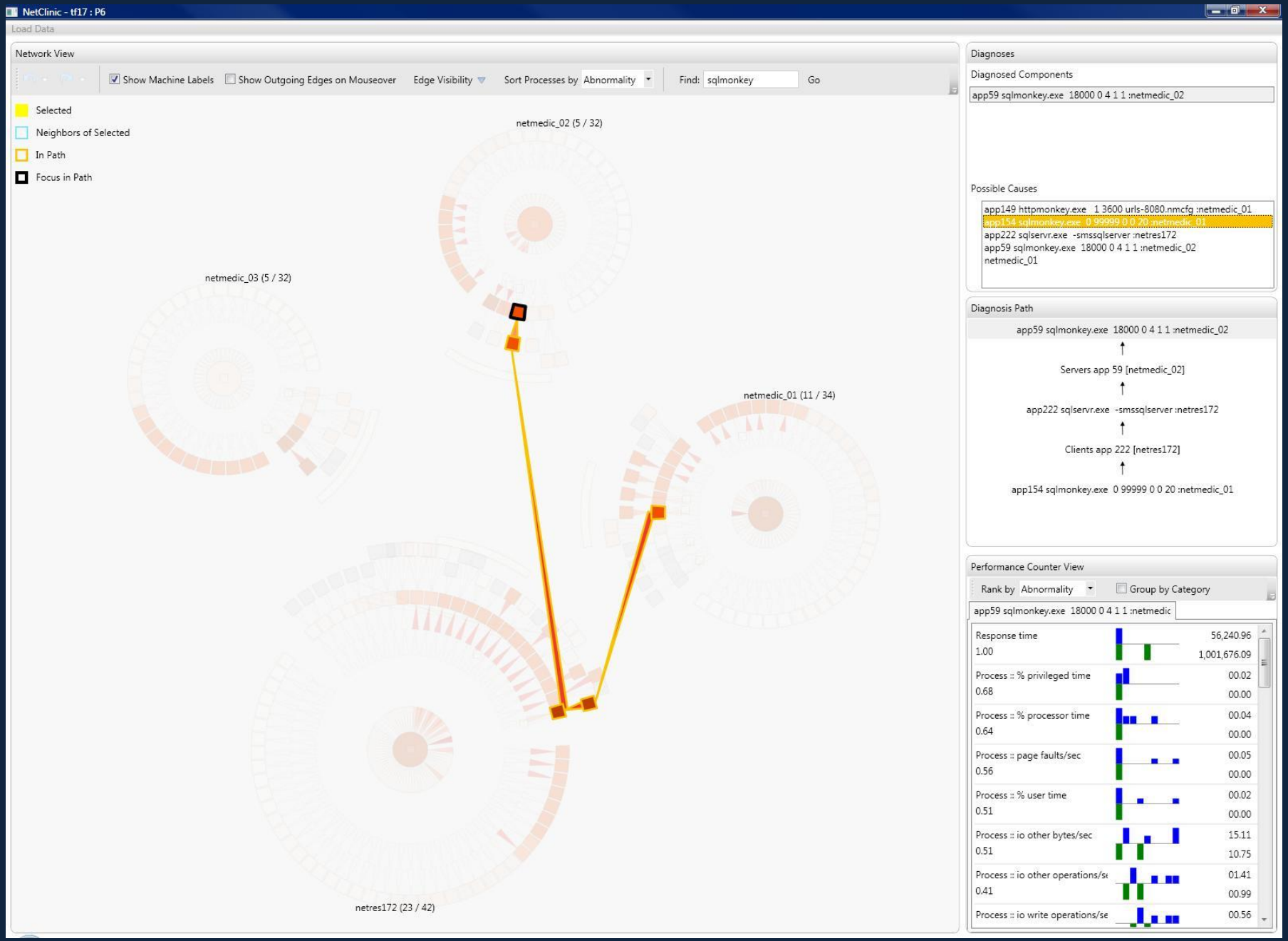
- Not much existing work; this uncertainty differs from that of typical scientific data
- Underlying assumption: humans can double check analysis if information is presented appropriately

An “HCI issue” that needs to be informed significantly by the underlying system structure


Dependency graph


NetClinic - tf17 : P6
Load Data
Network View
Show Machine Labels
Show Outgoing Edges on Mouseover
Edge Visibility
Sort Processes by Abnormality
Find:
Go
Selected
Neighbors of Selected
In Path
Focus in Path
netmedic_02 (5 / 32)
netmedic_03 (5 / 32)
netmedic_01 (11 / 34)
netres172 (23 / 42)
Diagnoses
Diagnosed Components
Possible Causes
Diagnosis Path
Performance Counter View
Rank by Abnormality
Group by Category

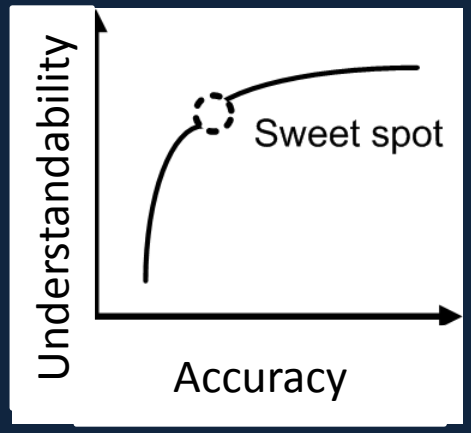

Top 10 culprits for app65 httpmonkey.exe 4 36000 urls-80.nmcfg :netmedic_02
app65 httpmonkey.exe 4 36000 urls-80.nmcfg :netmedic_02
0.80
Servers app 65 [netmedic_02]
0.80
<1> config :: app 267 [netres172]
app267 w3wp.exe -a iisipm4e2200aa-390a-4b53-a473-23b6def8d6b7 -v v2.0 -h c:\inetpub\temp\apppools\defaultapppool.config -w -m 0 -t 20 -ap defaultapppool :netres172
0.85
<6> app226 lsass.exe :netres172
<8> app204 svchost.exe -k netsvcs :netres172
<7> app200 store.exe :netres172
0.94
0.94
netres172
<2> app201 svchost.exe -k gpsvcgroup :netres172
<9> app262 microsoft.exchange.search.exsearch.exe :netres172
<10> app240 svchost.exe -k tapisrv :netres172
0.94
<3> app230 w3wp.exe -a iisipme76c6f11-5d58-47de-a4bd-0ccdcaa4db26 -v v2.0 -h c:\inetpub\temp\apppools\msexchangeowaapppool.config -w -m 1 -ap msexchangeowaapppool :netres172
<4> app232 microsoft.exchange.edgesyncsvc.exe :netres172
<5> app202 svchost.exe -k localservicenetworkrestricted :netres172


NetClinic - tf17 : P6
Load Data
Network View
Show Machine Labels
Show Outgoing Edges on Mouseover
Edge Visibility
Sort Processes by Abnormality
Find: sqlmonkey
Go
Selected
Neighbors of Selected
In Path
Focus in Path
netmedic_02 (5 / 32)
netmedic_03 (5 / 32)
netmedic_01 (11 / 34)
netres172 (23 / 42)
Diagnoses
Diagnosed Components
app59 sqlmonkey.exe 18000 0 4 1 1 :netmedic_02
Possible Causes
app149 httpmonkey.exe 1 3600 urls-8080.nmcfg :netmedic_01
app154 sqlmonkey.exe 0 99999 0 0 20 :netmedic_01
app222 sqlservr.exe -smssqlserver :netres172
app59 sqlmonkey.exe 18000 0 4 1 1 :netmedic_02
netmedic_01
Diagnosis Path
app59 sqlmonkey.exe 18000 0 4 1 1 :netmedic_02
Servers app 59 [netmedic_02]
app222 sqlservr.exe -smssqlserver :netres172
Clients app 222 [netres172]
app154 sqlmonkey.exe 0 99999 0 0 20 :netmedic_01
Performance Counter View
Rank by Abnormality
Group by Category
app59 sqlmonkey.exe 18000 0 4 1 1 :netmedic
Response time
1.00
56,240.96
1,001,676.09
Process :: % privileged time
0.68
00.02
00.00
Process :: % processor time
0.64
00.04
00.00
Process :: page faults/sec
0.56
00.05
00.00
Process :: % user time
0.51
00.02
00.00
Process :: io other bytes/sec
0.51
15.11
10.75
Process :: io other operations/s
0.41
01.41
00.99
Process :: io write operations/se
00.56

Intuitiveness of analysis

The ability to reason about the system's analysis

- A non-traditional dimension of system effectiveness
- Counters the tendency of optimizing the system for incremental accuracy



A "systems issue" that needs to be informed significantly by HCI

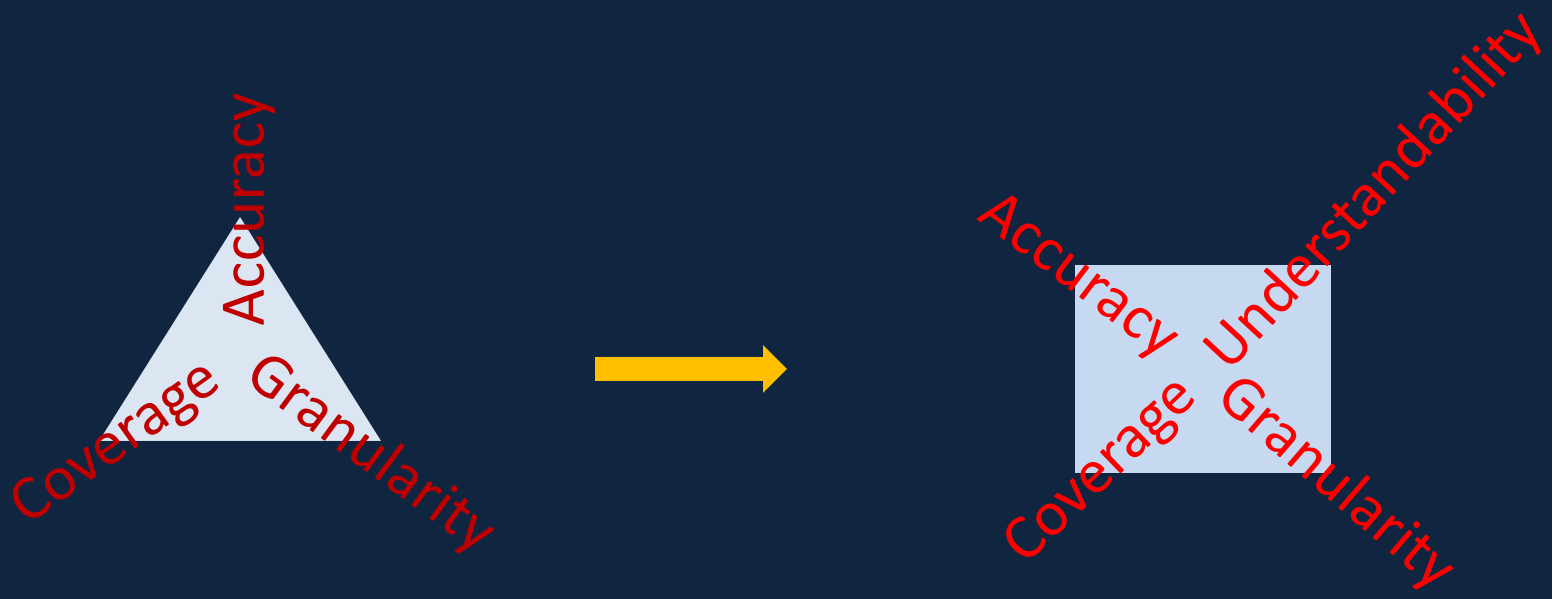
Intuitiveness of analysis (2)

Goal: Go from mechanical measures to more human centric measures

- Example: MoS measure for VoIP

Factors that should be considered

- What information is used?
  - E.g., Local vs. global
- What operations are used?
  - E.g., arithmetic vs. geometric means



Considerations for diagnostic systems