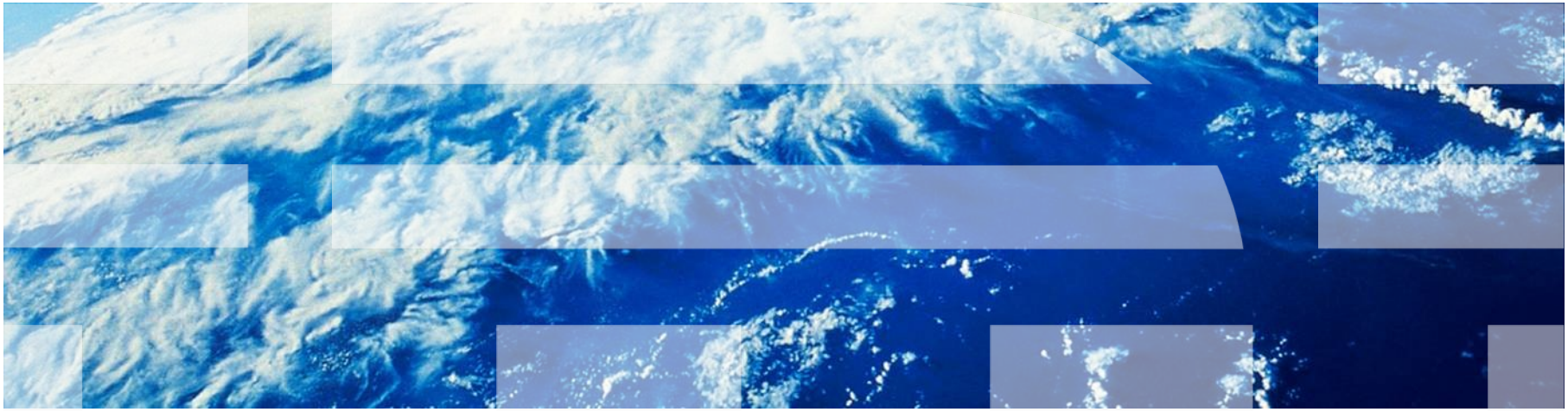
A Virtualization Assurance Language for Isolation and Deployment

Sören Bleikertz and Thomas Groß
IBM Research – Zurich



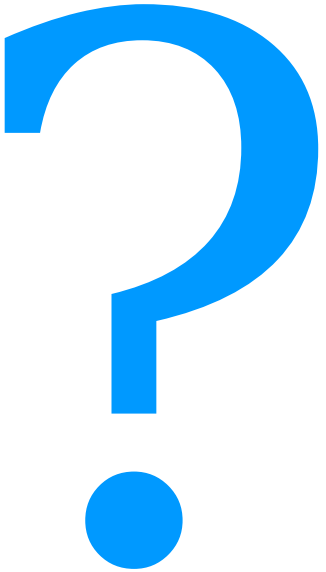
Why does it matter?

© 2011 IBM Corporation

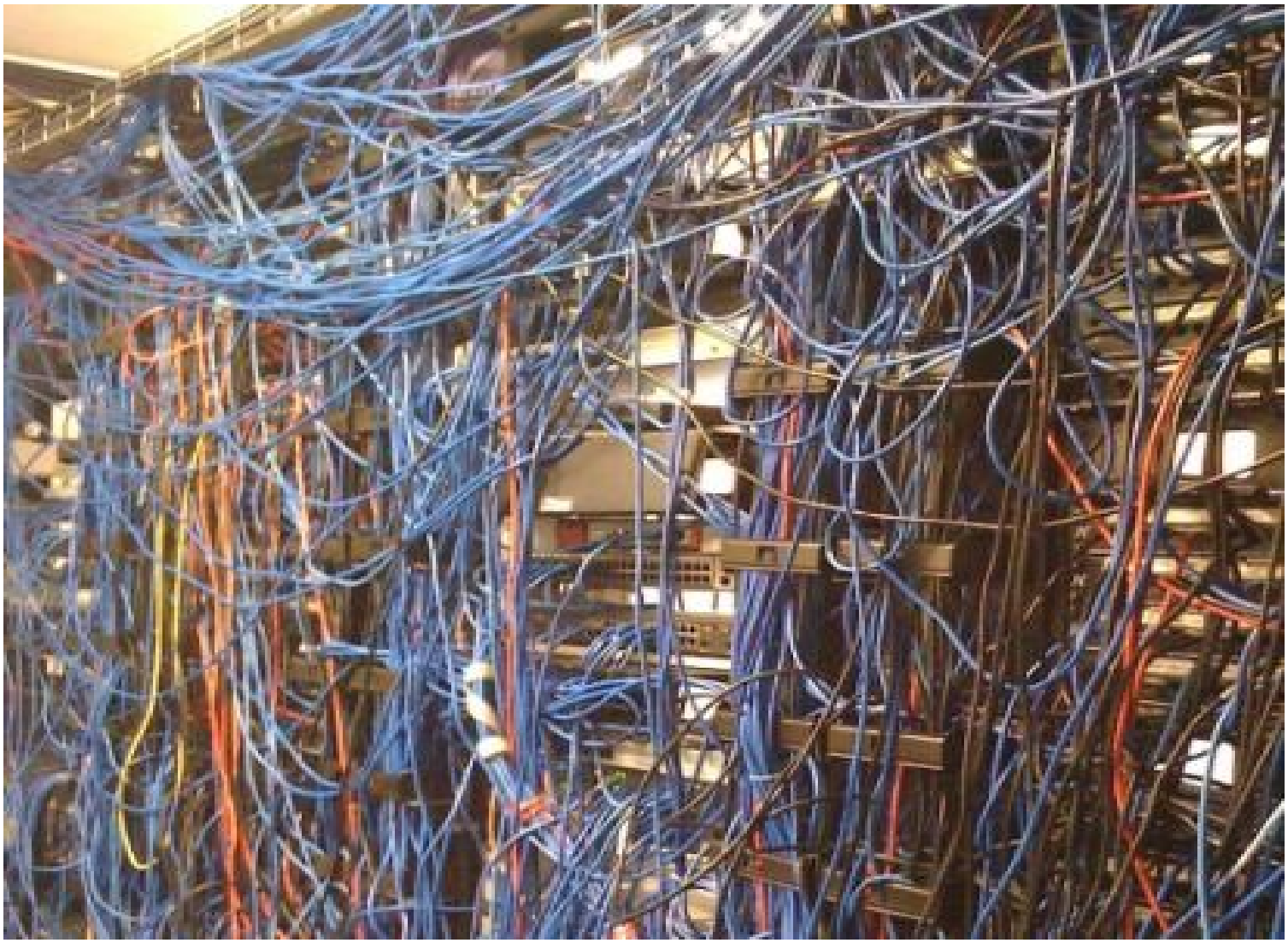
Is my data accessible by other tenants

Is my workload running on the appropriate hosts

What happens when a host fails



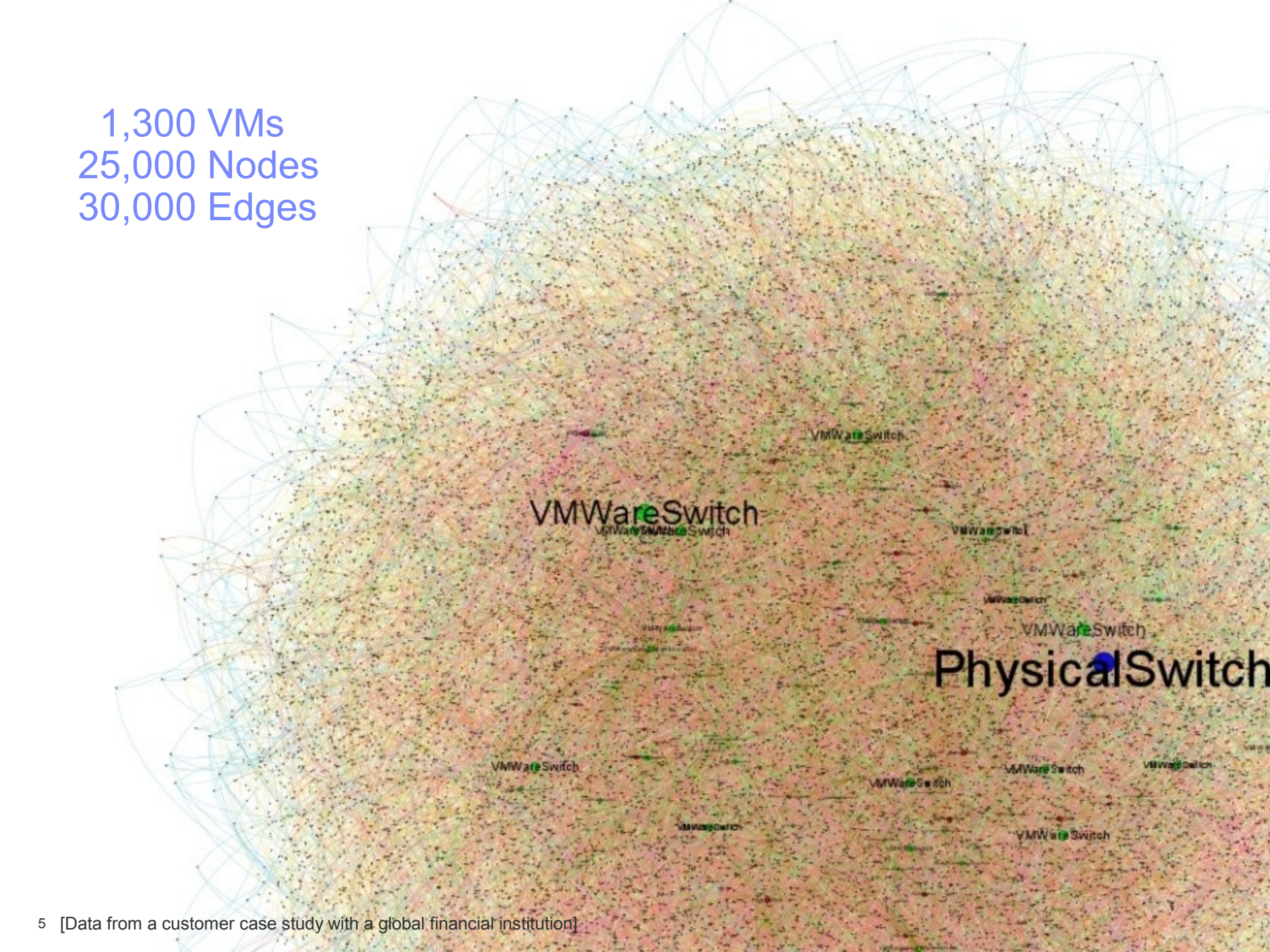
© 2011 IBM Corporation



“Days of a startup”
http://www.flickr.com/photos/tangysd/

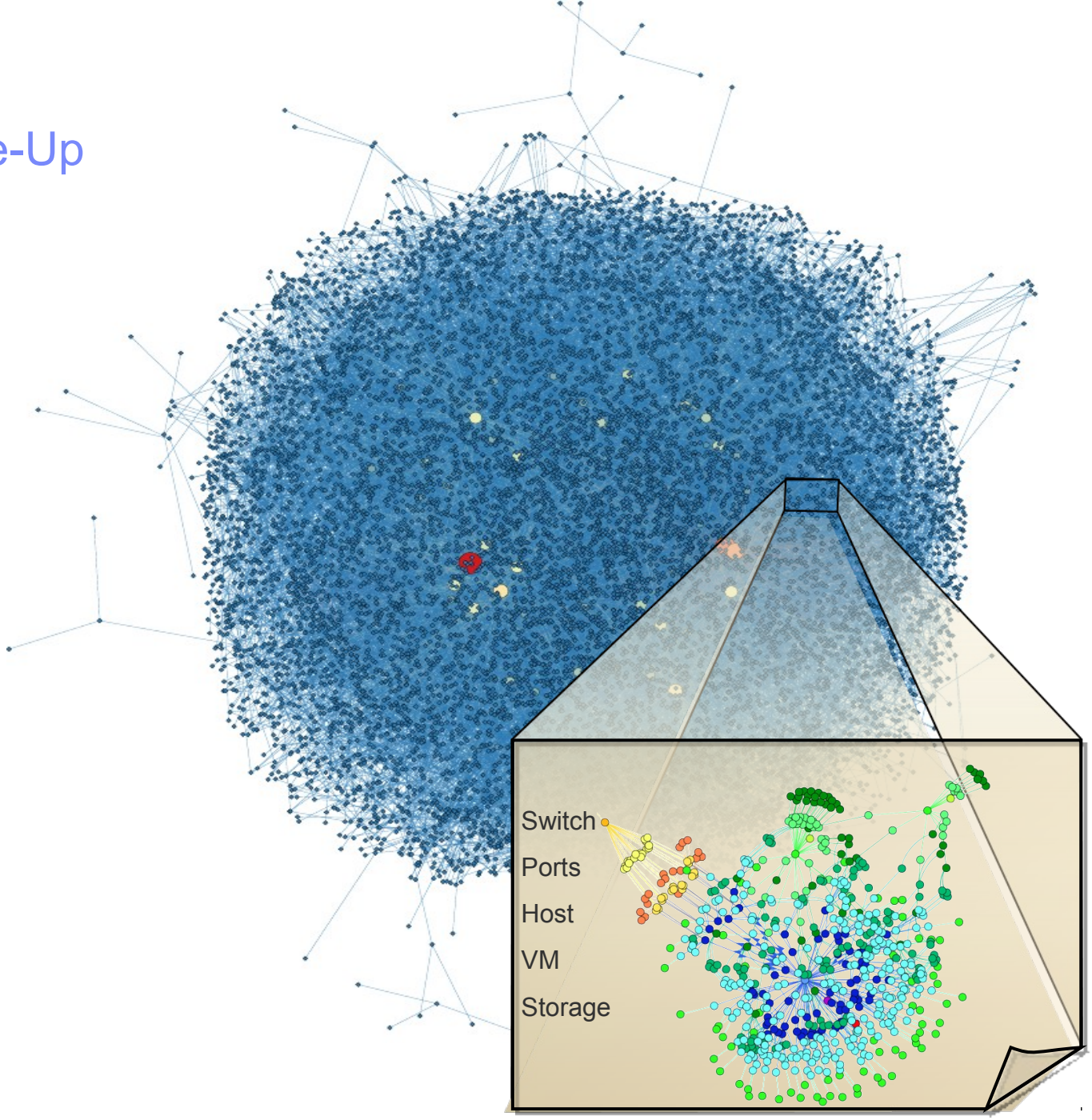
© 2011 IBM Corporation

1,300 VMs
25,000 Nodes
30,000 Edges



 [Data from a customer case study with a global financial institution]

Close-Up



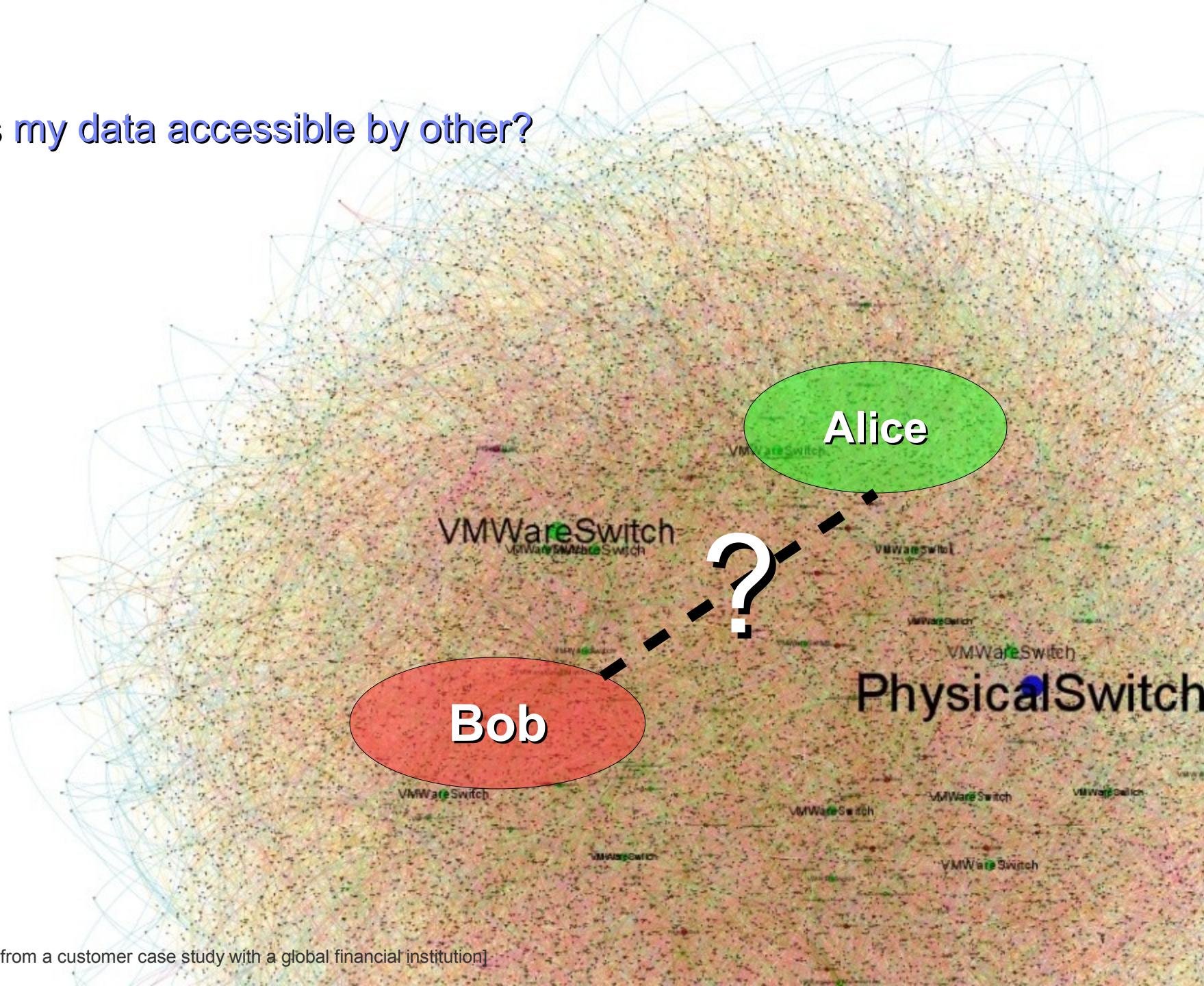
We need automated tools!

© 2011 IBM Corporation

How to specify security goals?

© 2011 IBM Corporation

Is my data accessible by other?



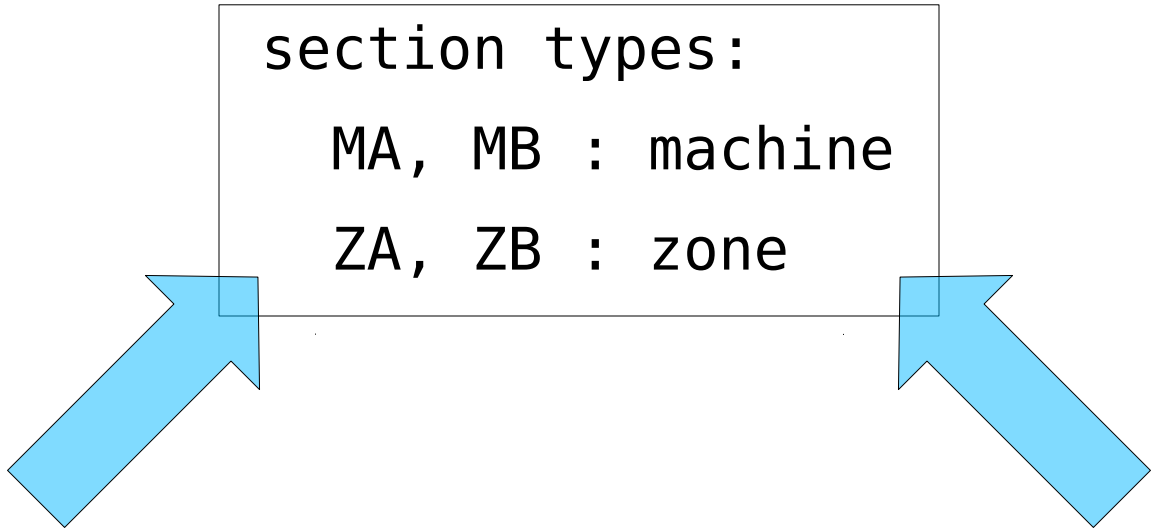
 [Data from a customer case study with a global financial institution]

Policy Specification: Zone Isolation

```
section types:
  MA, MB : machine
  ZA, ZB : zone

section goals:
  goal isolationBreach (info; ZA, ZB, MA, MB) :=
    contains (ZA, MA).contains (ZB, MB)
    .connected (MA, MB)
    & not(equal(ZA, ZB))
```


© 2011 IBM Corporation

Term Algebra and Atomic Terms



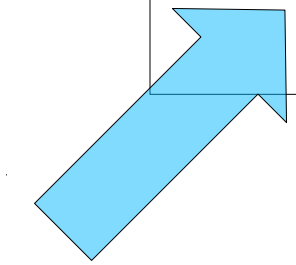
Variables: MA, MB..
Constants: ma, mb

Type System:
machine, zone,
node, hypervisor..

© 2011 IBM Corporation

Term Algebra and Atomic Terms

```
section goals:

  goal isolationBreach
  (info; ZA, ZB, MA, MB) :=

    ...
```

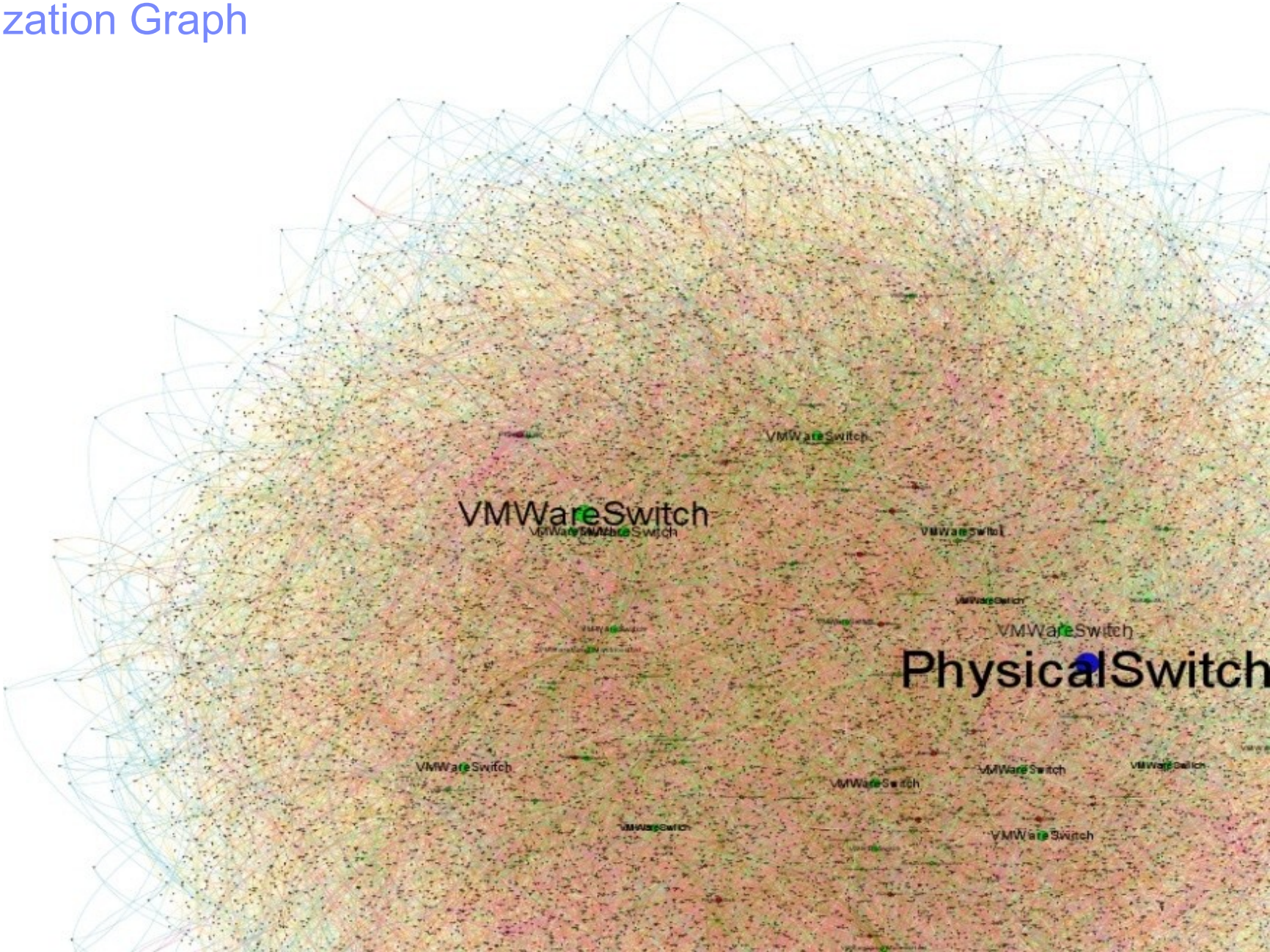


Graph Types:

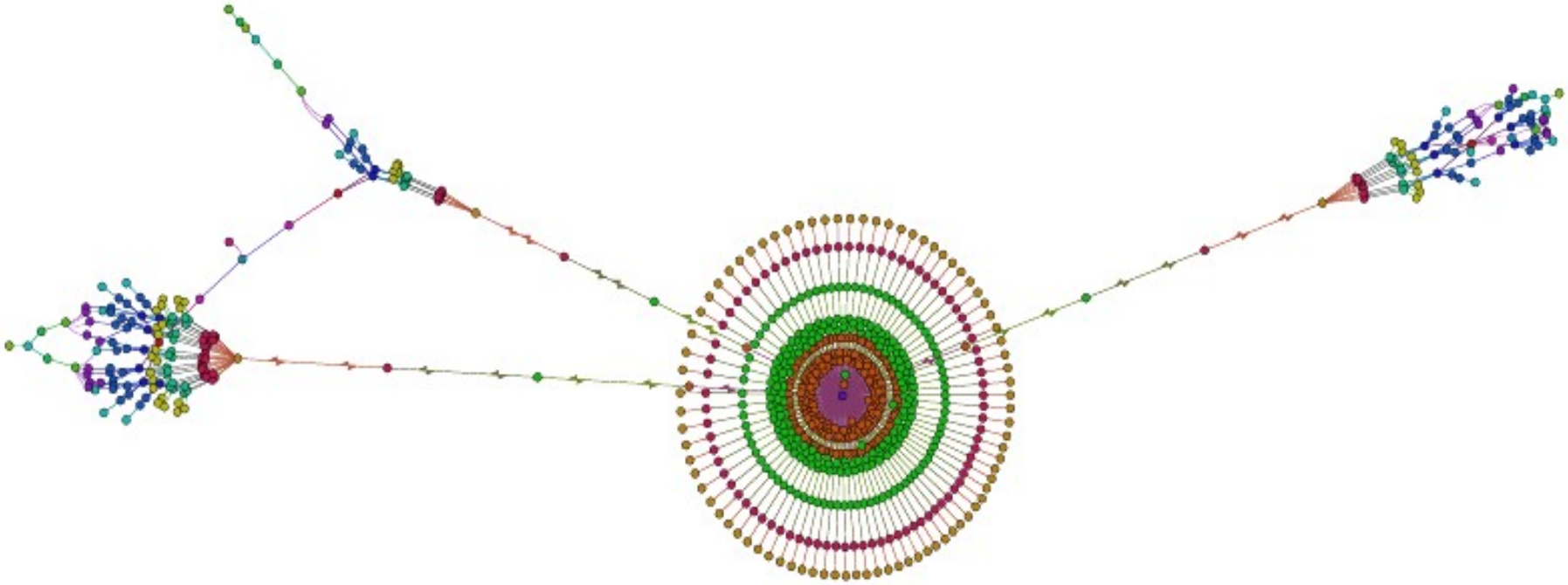
`real, info, depend`

© 2011 IBM Corporation

Realization Graph



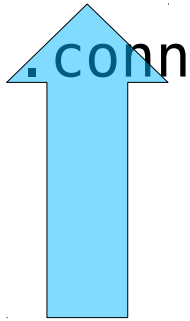
Information Flow Graph



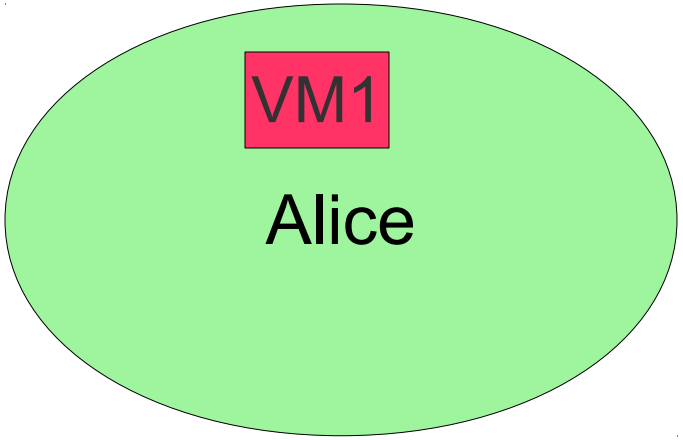
© 2011 IBM Corporation

Function Symbols

```
goal isolationBreach (info; ZA, ZB, MA, MB) :=
    contains (ZA, MA).contains (ZB, MB)
    .connected (MA, MB) & not(equal(ZA, ZB))
```



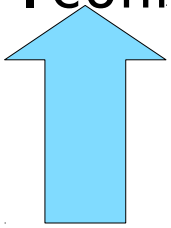
```
contains (S, E)
```



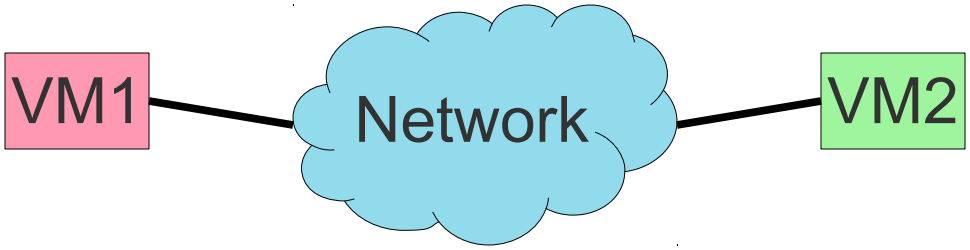
© 2011 IBM Corporation

Function Symbols

```
goal isolationBreach (info; ZA, ZB, MA, MB) :=
    contains (ZA, MA).contains (ZB, MB)
    .connected (MA, MB) & not(equal(ZA, ZB))
```



```
connected ([G : real], A, B)
```



© 2011 IBM Corporation

More Function Symbols

```
edge ([G : real], A, B)
paths ([G : real], A, B)
..
```


© 2011 IBM Corporation

Facts, State, Conditions

```
goal isolationBreach (info; ZA, ZB, MA, MB) :=
    contains (ZA, MA).contains (ZB, MB)
    .connected (MA, MB) & not(equal(ZA, ZB))
```

- Fact: `contains (ZA, MA)`
- State: `contains().contains().connected()`
- Condition: `not(equal(ZA, ZB))`

© 2011 IBM Corporation

Goals

```
section goals:
goal isolationBreach (info; ZA, ZB, MA, MB) :=
    contains (ZA, MA).contains (ZB, MB)
    .connected (MA, MB) & not(equal(ZA, ZB))
```


© 2011 IBM Corporation

Variety of Security Goals

Single Point of Failure

```
section types:
  M                              : machine
  NA, NB                         : network
  C                              : class

section goals:
goal singlePoF_Net (depend; NA,NB,M,C) :=
  contains(C,NA).contains(C,NB).connected(M,NA)
  not(connected(M,NB))
```

Zoning Breach

```
section types:
  MA, MB                         : machine
  subsection idealTypes:
    ZA, ZB                       : zone
  subsection realTypes:
    ZA0, ZB0                     : zone

section goals:
goal zoningBreach_Missing (info; ZA,ZA0,MA) :=
  matches(ZA,ZA0).contains(ZA,MA).
    not(contains(ZA0,MA))
goal zoningBreach_Unknown (info; ZB,ZB0,MB) :=
  matches(ZB,ZB0).not(contains(ZB,MB)).
    contains(ZB0,MB)
```

Deployment Breach

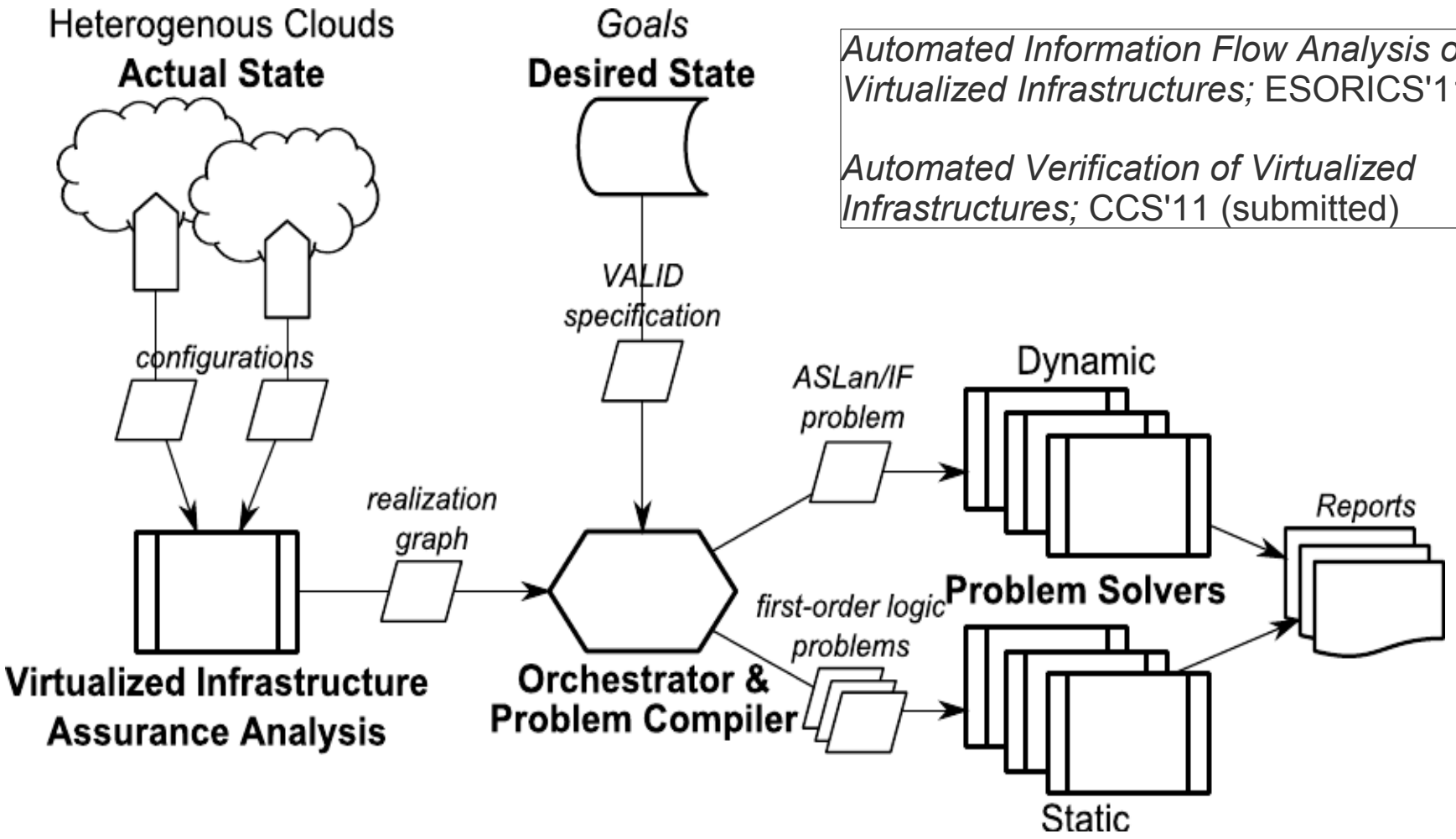
```
section types:
  M                              : machine
  subsection idealTypes:
    HA                           : host
  subsection realTypes:
    HB                           : host

section goals:
goal deploymentBreach (real; HA,HB,M) :=
  not(matches(HA,HB)).edge(HA,M).edge(HB,M)
```


© 2011 IBM Corporation

How to validate a policy?

© 2011 IBM Corporation

Outlook: Integration with SAVE



Automated Information Flow Analysis of Virtualized Infrastructures; ESORICS'11

Automated Verification of Virtualized Infrastructures; CCS'11 (submitted)

© 2011 IBM Corporation

Conclusion

- Virtualized infrastructures are complex
- Assurance language usable with automated tools
- Expressing a variety of security goals

- More information in the paper!

© 2011 IBM Corporation

Questions?

© 2011 IBM Corporation