A Virtualization Assurance Language for Isolation and Deployment

Sören Bleikertz and Thomas Groß

*IBM Research – Zurich*
Why does it matter?
Is my data accessible by other tenants

Is my workload running on the appropriate hosts

What happens when a host fails
“Days of a startup”
http://www.flickr.com/photos/tangysd/
1,300 VMs
25,000 Nodes
30,000 Edges

[Data from a customer case study with a global financial institution]
We need automated tools!
How to specify security goals?
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))
Term Algebra and Atomic Terms

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

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

Type System:
machine, zone, node, hypervisor..
Term Algebra and Atomic Terms

section goals:

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

Graph Types:
real, info, depend
Realization Graph
Information Flow Graph
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)
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)
More Function Symbols

\[ \text{edge ([G : real], A, B)} \]
\[ \text{paths ([G : real], A, B)} \]

..
goal isolationBreacht (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))
goals isolation Breach (info; ZA, ZB, MA, MB) :=
  contains (ZA, MA).contains (ZB, MB)
  .connected (MA, MB) & not(equal(ZA, ZB))
Variety of Security Goals

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

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

Single Point of Failure

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)

Zoning 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)

Deployment Breach
How to validate a policy?
Outlook: Integration with SAVE

Automated Information Flow Analysis of Virtualized Infrastructures; ESORICS'11

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

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

- More information in the paper!
Questions?