Icebergs in the Clouds:
the *Other* Risks of Cloud Computing

Bryan Ford
Yale University
http://dedis.cs.yale.edu/

position paper:
http://arxiv.org/abs/1203.1979

NSF Cloud Security Workshop, March 16, 2012

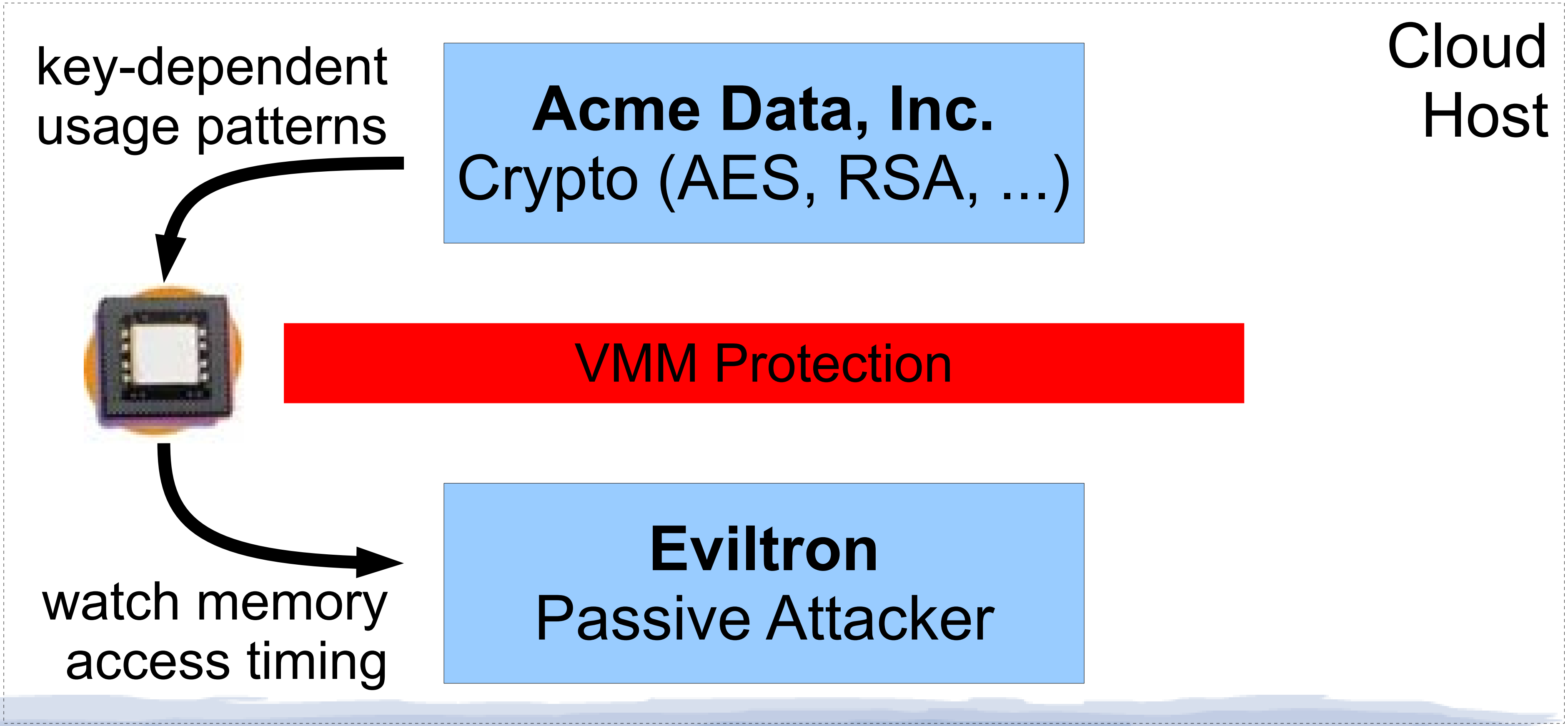
Well-Known, “Immediate” Risks

- Traditional Information Security
  - Security of data
  - Integrity of data, computation
  - Personal privacy
  - Malware defense
  - Availability, reliability
  - …
- Important, plenty more to be done, but *not what this talk is about*

What risks *might* appear that we're not looking at yet/enough?

Four potential risks...

1. Side-Channels



Cloud Host

key-dependent usage patterns

Acme Data, Inc.
Crypto (AES, RSA, ...)

VMM Protection

Eviltron
Passive Attacker

watch memory access timing

Timing Channels

The cloud *exacerbates* timing channel risks:

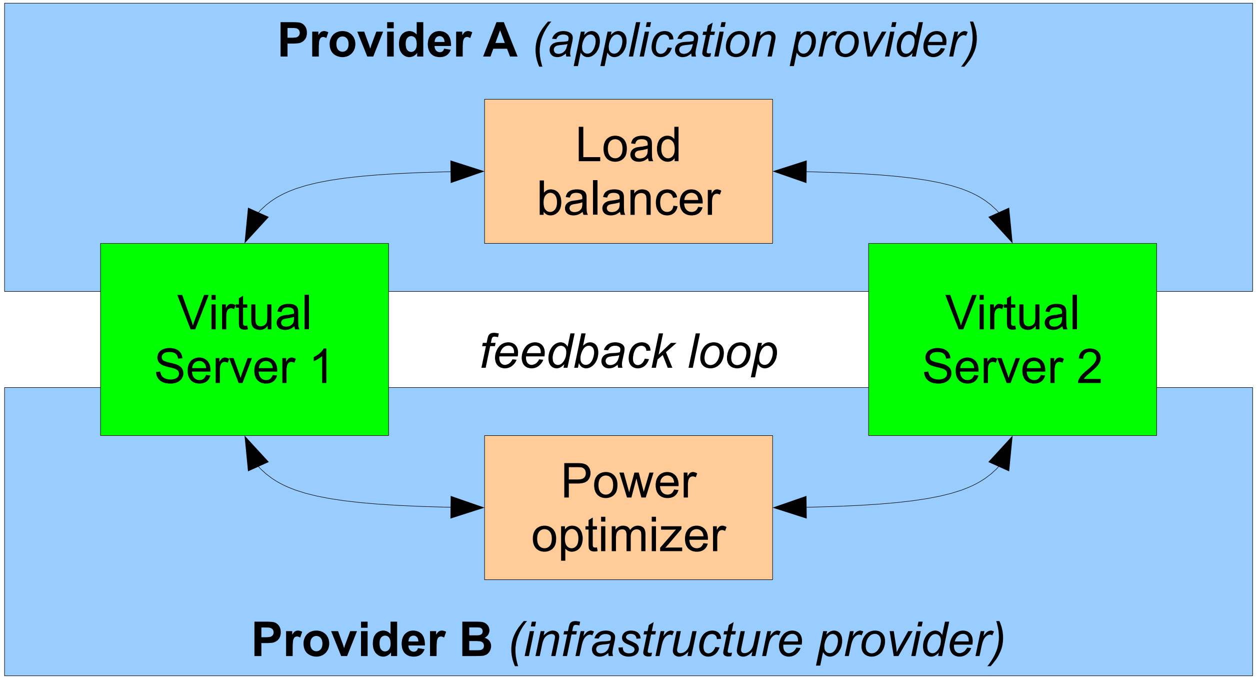
1. Routine co-residency
2. Massive parallelism
3. No intrusion alarms → hard to monitor/detect
4. Partitioning defenses defeat elasticity

“*Determinating Timing Channels in Compute Clouds*” [CCSW '10]

What risks *might* appear that we're not looking at yet/enough?

Four potential risks...

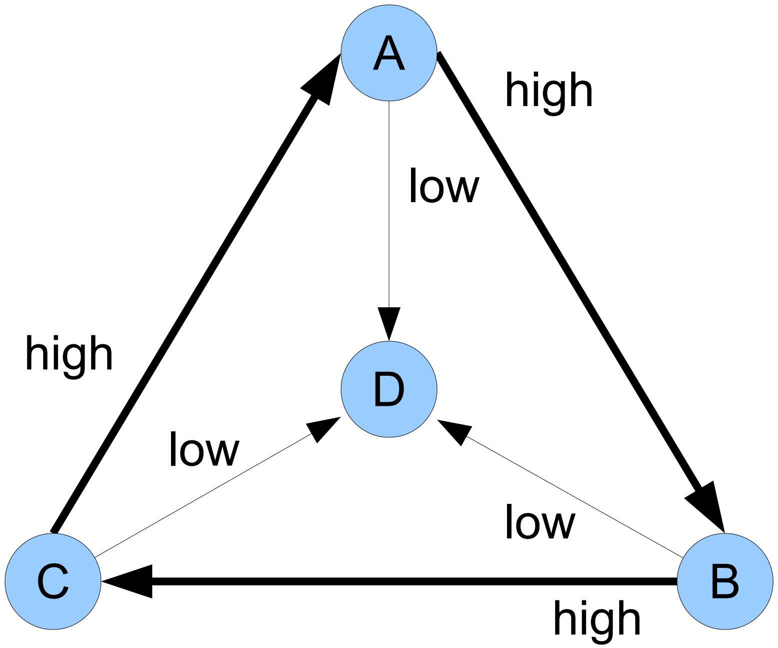
1. Side-Channels
2. Reactive Stability


Provider A *(application provider)*
Load balancer
Virtual Server 1
feedback loop
Virtual Server 2
Power optimizer
Provider B *(infrastructure provider)*

Seen this before?

BGP “dispute wheel”

- uncoordinated policies can loop



In the Cloud:

- providers want max usage, profit → *oversubscribe*
- handle overloads → *swap with peers?*

Cloud dispute wheels?

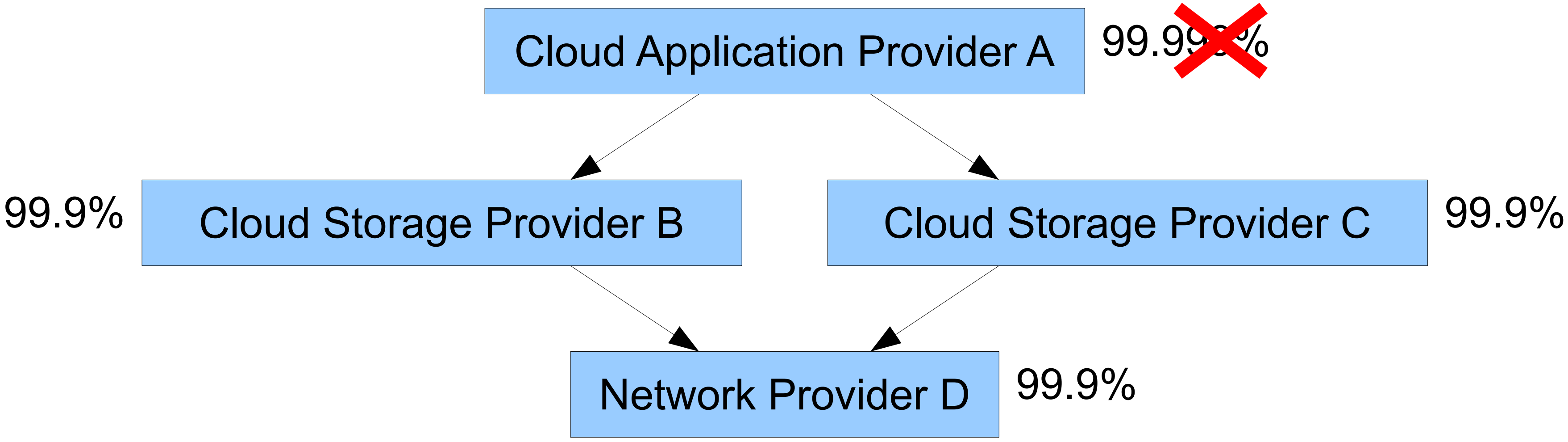
Credit default swaps?

Speculation, bubbles?

What risks *might* appear that we're not looking at yet/enough?

Four potential risks...

1. Side-Channels
2. Reactive Stability
3. Cross-Layer Robustness



Cloud Application Provider A 99.999%

99.9% Cloud Storage Provider B

Cloud Storage Provider C 99.9%

Network Provider D 99.9%

What risks *might* appear that we're not looking at yet/enough?

Four potential risks...

1. Side-Channels
2. Reactive Stability
3. Cross-Layer Robustness
4. *Are We the Bad Guys?*

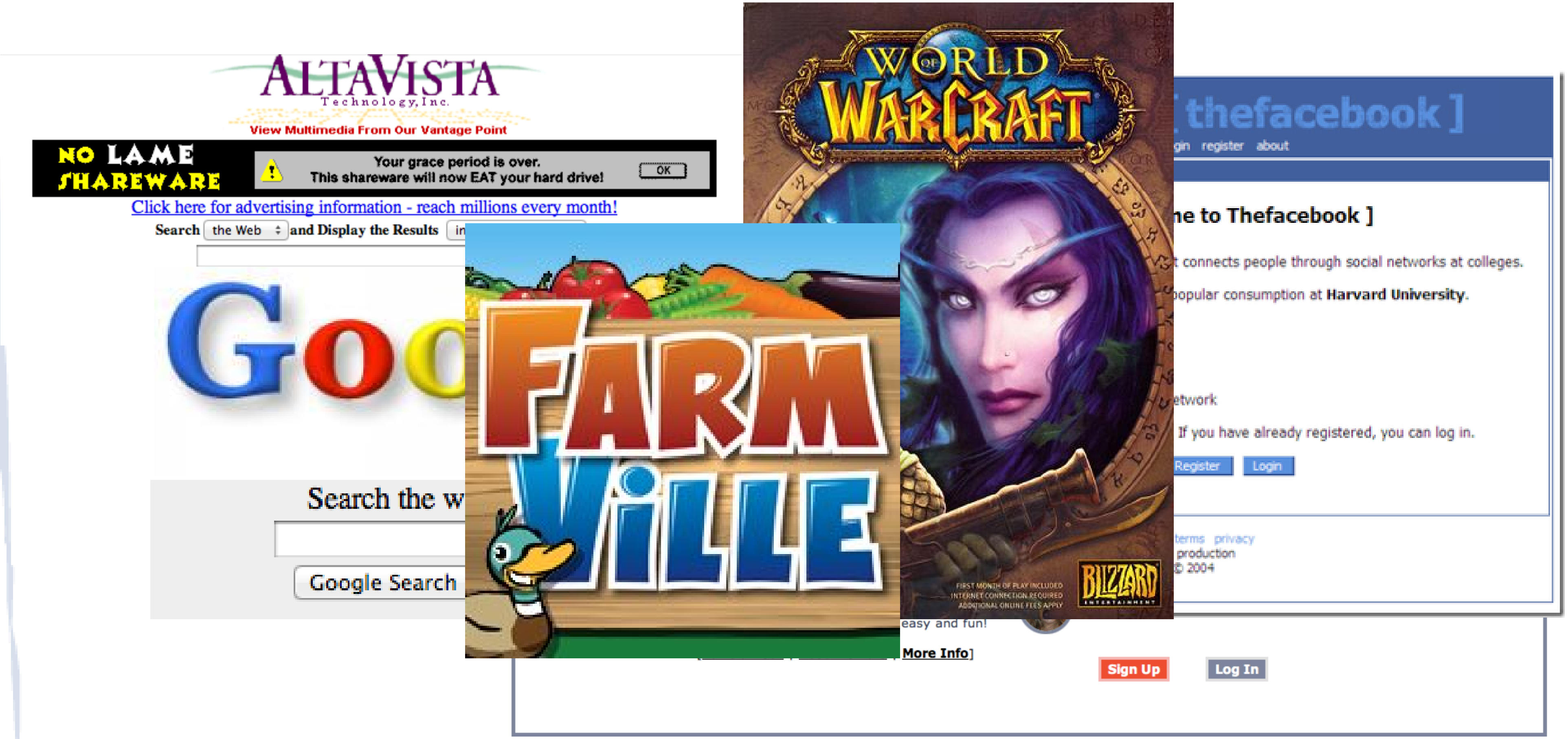
In 1000 years...

Someone will still have a copy of:

THE
ILIAI
OF
HOME
TRANSLATED AND WITH AN INTRODUCTION BY
RICHMOND LATTIMORE
Adam Smith
AN INQUIRY
INTO THE
NATURE AND CAUS
OF THE
WEALTH OF NATION
Volume I
Elibron Classics
STAR WARS
TRILOGY
A NEW HOPE
LET IT BE
PACM
SCORE 24570
LIVES
DOOM
id

In 1000 years...

Will *anyone* still have a usable “copy” of:



Your grace period is over.
This shareware will now EAT your hard drive!

Click here for advertising information - reach millions every month!

Search the Web and Display the Results in

ne to Thefacebook]

t connects people through social networks at colleges.

popular consumption at **Harvard University**.

etwork

If you have already registered, you can log in.

production
© 2004

easy and fun!

A Darker Digital Dark Age?

- Many culturally important artifacts are and will *increasingly* be cloud-based apps & services
- *No one* but the app/service provider has code & data necessary to preserve history
  - Does the Library of Congress have a copy of Google 1.0? Facebook 1.0? WoW 1.0?
- What about the blogs, tweets, or email records of the next Homer/Newton/Marx/Einstein?
- *Cloud artifacts are naturally non-preservable*

What risks *might* appear that we're not looking at yet/enough?

Four potential risks...

1. Side-Channels
2. Reactive Stability
3. Cross-Layer Robustness
4. Digital Preservation

...and no doubt not the end of the list!

Conclusion

What are the risks beyond information security?

What could happen if we don't address them?

“Icebergs in the Clouds”

http://arxiv.org/abs/1203.1979

Bryan Ford – Yale DeDiS group

http://dedis.cs.yale.edu