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

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

USENIX HotCloud, June 12, 2012

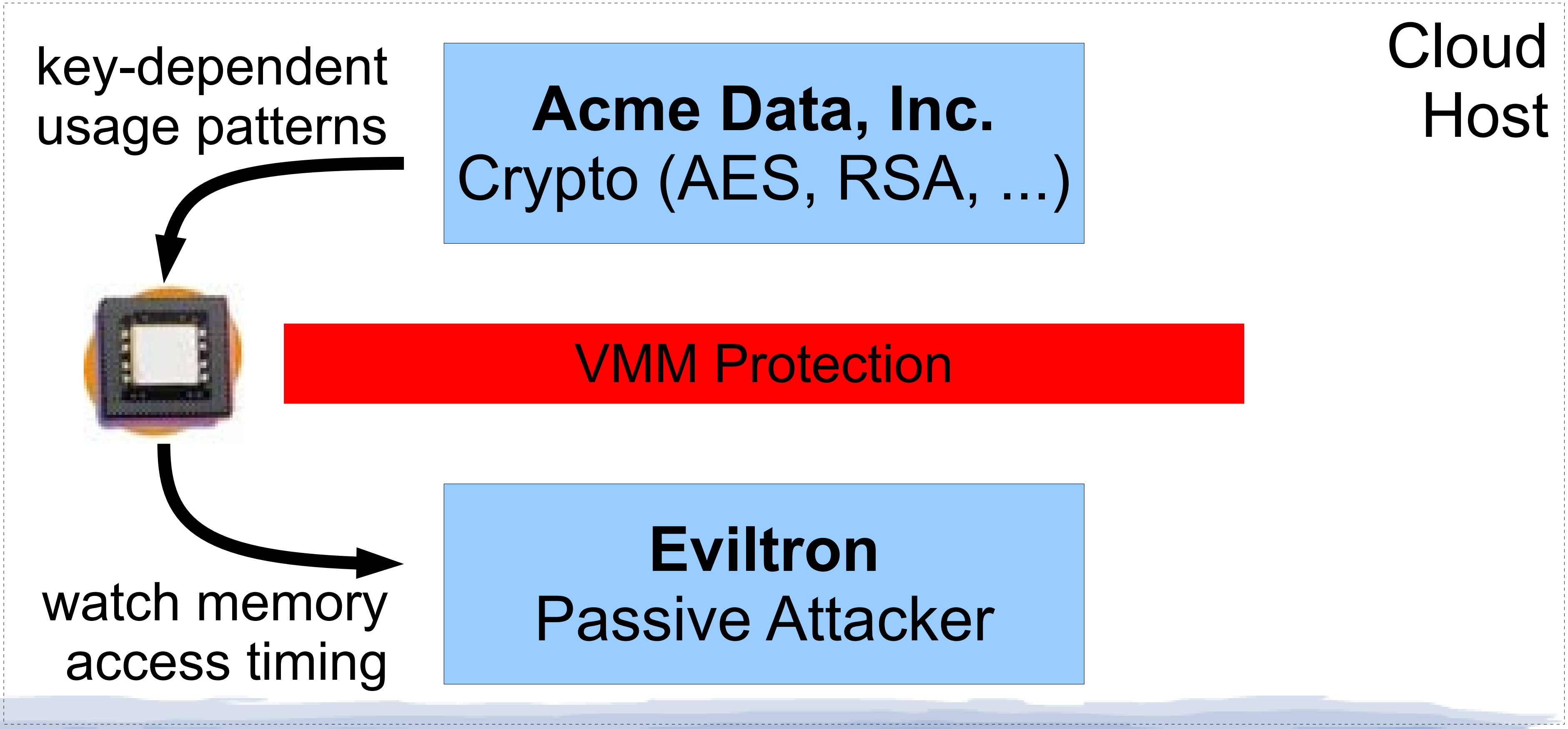
Well-Known, “Immediate” Risks

- 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?

Several potential risks...

1. **Side-Channels**



Timing Channels

The cloud *exacerbates* timing channel risks:

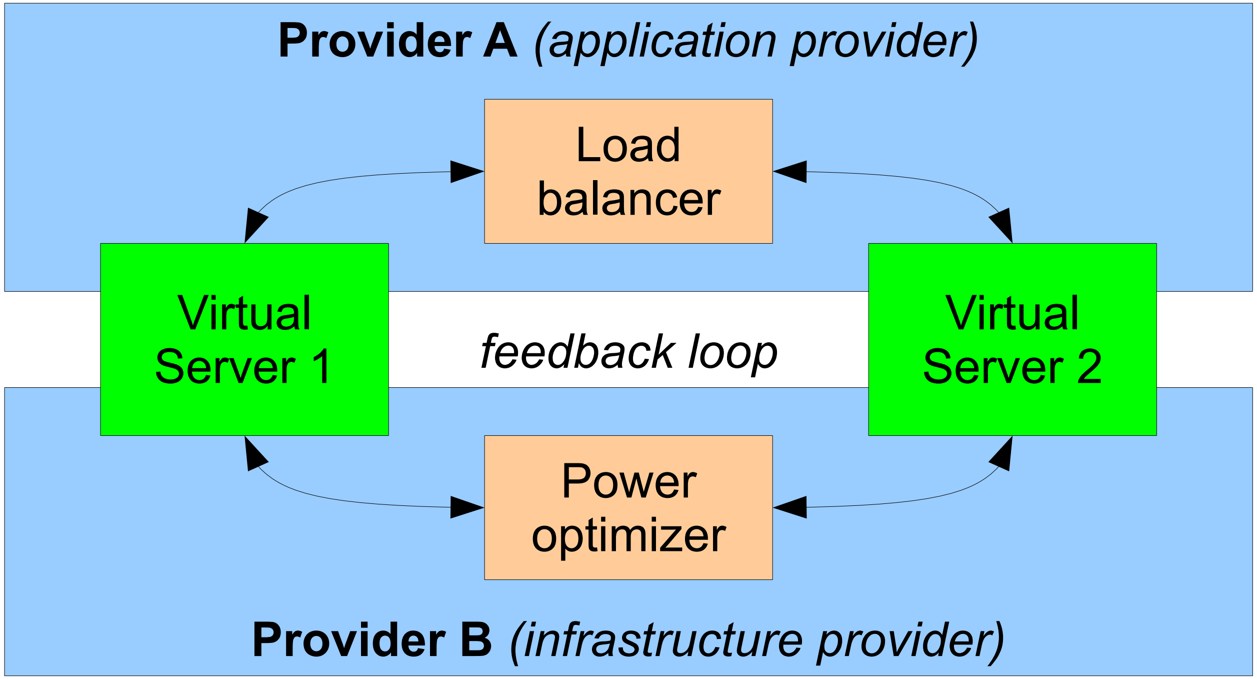
1. Routine co-residency
2. Massive parallelism
3. No intrusion alarms → hard to monitor/detect
4. Partitioning defenses defeat elasticity

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

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

Several potential risks...

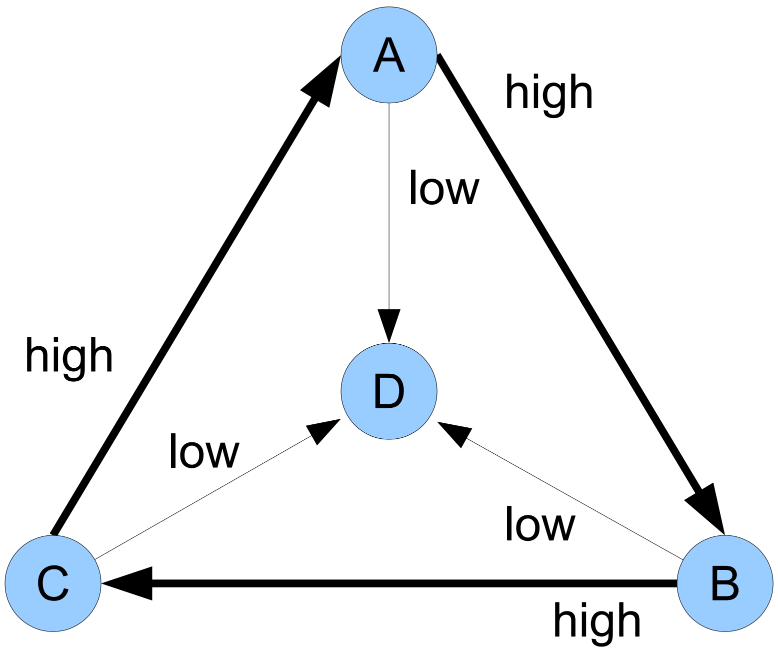
1. Side-Channels
2. **Reactive Stability**


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:

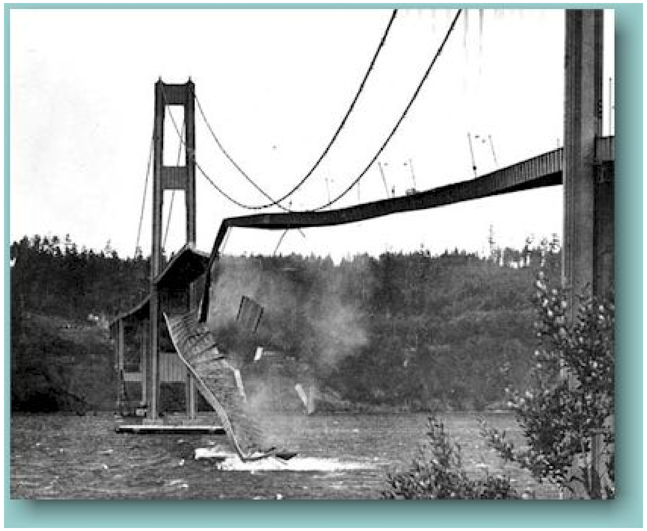
- providers want max usage, profit → *oversubscribe*
- handle overloads → *swap with peers?*

Cloud dispute wheels?

Credit default swaps?

Speculation, bubbles?

Weather Forecast

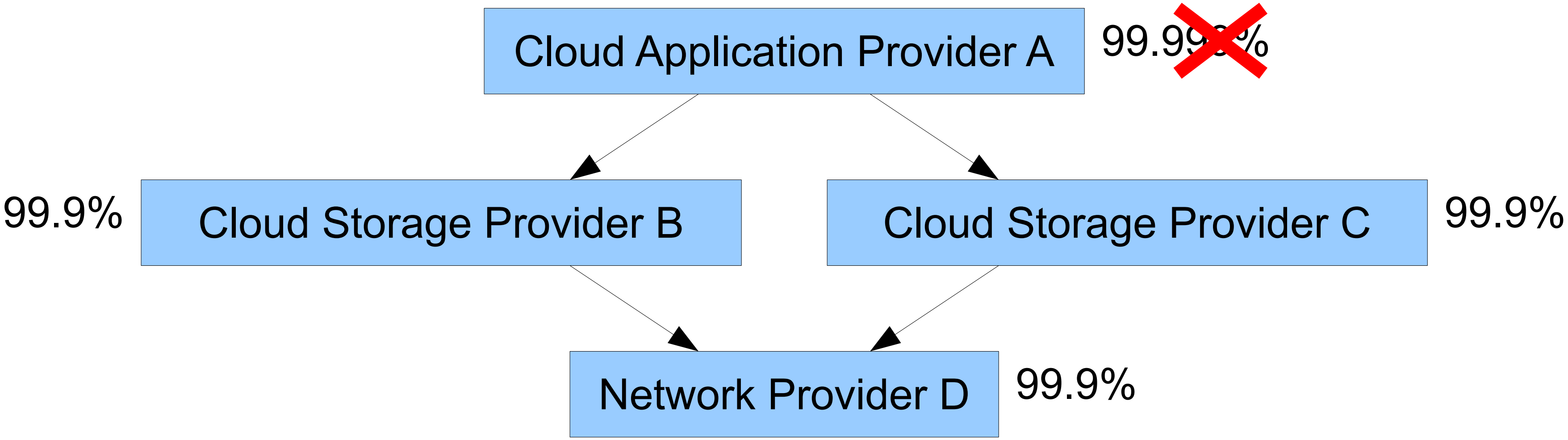


- Cloudy with a chance of
  - Wild instabilities
  - Occasional collapses
- Accidents *already* happen
  - Mogul, “Emergent (mis)behavior…” [EuroSys'06]
- But cloud computing makes this risk *systemic*
  - Control theory might help *given information*
  - But incentives to keep algorithms secret
    → *no one* can analyze across providers!

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

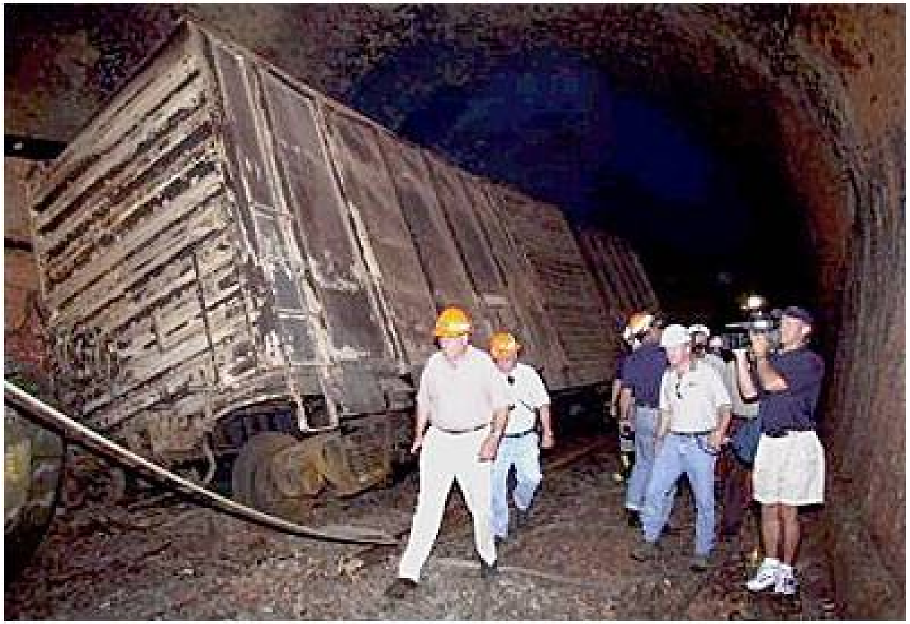
Several potential risks...

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



Correlated Failures Already Happen

- Baltimore Howard Street Tunnel Fire of 2001
  - Cut a bundle of fibre optic cables serving *several* major ISPs simultaneously
  - Risk wasn't apparent until train blew up



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

Several potential risks...

1. Side-Channels
2. Reactive Stability
3. Cross-Layer Robustness
4. **The Always-Connected Assumption**

Ender's Game: the “Hive Mind”

~~THEM~~

US

~~US~~

Mother Nature

A Disaster-Readiness Disaster

- The cloud model *assumes* “always-connected”
  - But in any disaster, connectedness is first to go
- Can't lookup “CPR instructions” on Wikipedia
- Can't find road out of town with Maps app
- Siri may be optional now, but for how long?
  - Can't launch “flashlight app” or “compass app”
- What happens to search/rescue drones without their ground-based logic, operators?

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

Several potential risks...

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

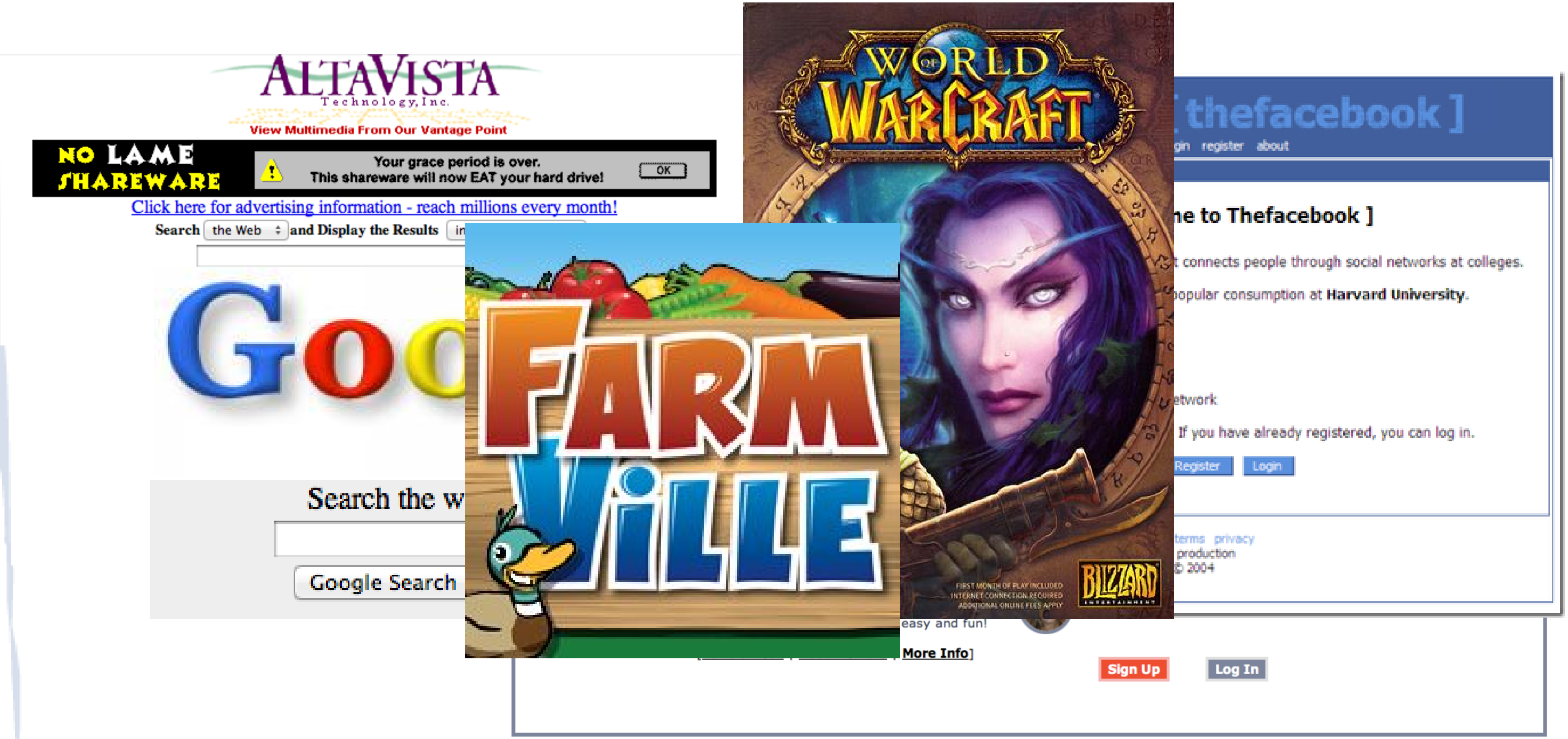
In 1000 years...

Someone will still have a copy of:

THE ILIAD OF HOMER
TRANSLATED AND WITH AN INTRODUCTION BY RICHMOND LATTIMORE
Adam Smith
AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS
Volume I
Elibron Classics
STAR WARS TRILOGY
A NEW HOPE
LET IT BE
PACMAN
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.

easy and fun!

Non-Preservability of the Cloud

Conventional artifacts have a ***decentralized preservability*** property

- Book/music/video producers *must* make “complete copies” available to customers
- Customers can work together to preserve

Cloud-based artifacts ***destroy*** this property

- *No one* but the app/service provider ever has code & data necessary to preserve history

A Darker Digital Dark Age?

Many culturally important artifacts are and will *increasingly* be cloud-based apps & services

- But *only* the provider can preserve them, and usually have few/no incentives to
- Does the Library of Congress, or *anyone*, have Google 1.0? Facebook 1.0? WoW 1.0?
- What about the blogs, tweets, or email records of the next Homer/Newton/Marx/Einstein?

Will cloud artifacts be the next “hole” in history?

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

At least five potential risks...

1. Side-Channels
2. Reactive Stability
3. Cross-Layer Robustness
4. The Always-Connected Assumption
5. Non-Preservability of the Cloud

...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?

What research should we do to address them?

Bryan Ford – Yale DeDiS group

http://dedis.cs.yale.edu