Securing the Grid

Dan Geer
geer@stake.com
+1.617.768.2723

What grid computing needs

- Reliability
- Location independence
- Economy
- Metrics

To get those needs...

- Security is a subset of reliability
- Location independence is the focal point
- Economics ultimately rules
- Measurability by design is the only answer

Security $\subseteq$ Reliability

premise

If a system is insecure, then
It is unreliable, therefore
Security is necessary for reliability, yet
Security is insufficient for reliability, therefore
Security is a subset of reliability.

consequence

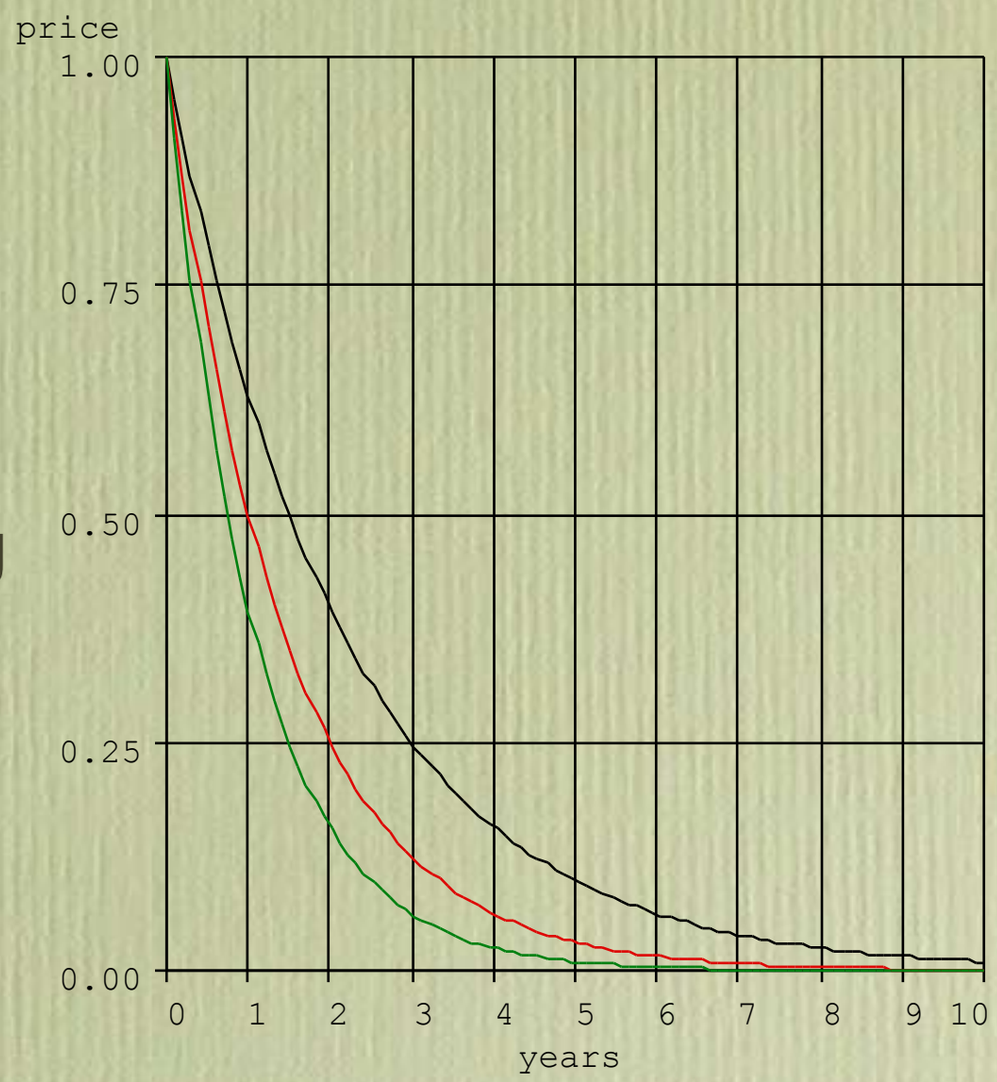
Mine the quality control literature

Location independence

- Location independence has driven everything for a decade and remains a goal
- Something has to move:
  move computing to where the data is
  move data to where the computing is
- But the more that is in motion,
  the more that is at risk

Economics = f(technology)

- Moore’s Law, 18mo doubling
- Storage, 12mo doubling
- Bandwidth, 9mo doubling



So is this hard or not?

Core security requirements

- More of the same -- but a lot more
- Integrity of host and results
- Verifiable metering
- Confidentiality -- of action as much as data

And research-grade problems do exist...

- Grid provider protects self from customer
- Grid provider protects customer from self
- Who protects $Customer_a$ from $Customer_b$?

Well, is it tractable?

Applications and Security

- Applications are where the action is now
- Especially relevant for grids
- Trends are worrying...
  ...but at least we can see them

Application security

should do
but doesn't

does do but
shouldn't

design

implementation

What factors matter?

factor 1 - *Applications are federating*

- Distributed applications have multiple security domains
  - The firm: client service & administrative functions
  - External providers: front-end Web farms and application hosting
  - Partner interfaces: data streams (inventory, payment, real-time feeds)
- Applications get ever more moving parts
  - Mainframe → client-server → n-tier → Model 2 (J2EE & .Net)
- Network service stratification
  - Bandwidth, hosting, provisioning, delivery

factor 2 - *Perimeter defense diseconomic*

- "Shared wire" supplants "shared model"
  - XML is the great equalizer
  - SOAP and XML-RPC specifically designed to go through firewalls
  - Emerging web services
- Firewalls stop nuisance attacks, not application traffic
  - Everyone leaves ports 80 and 443 open
- As a result, the threat model mutates
  - More attacks through HTTP, at application level
  - More attacks targeted at specific application components
  - Attacks on applications require lower skill levels

factor 3 - *Data, data everywhere*

- Data storage needs increasing quickly
  - More new data produced in next 3 years than in all of human history
  - Corporate IT spending on storage:
    4% in 1999 v. 17% in 2003 (Forrester)
- Form factors proliferating
  - Local storage
  - Storage arrays
  - Appliances/network-attached storage
  - COTS: <$1/GB, >100TB/rack

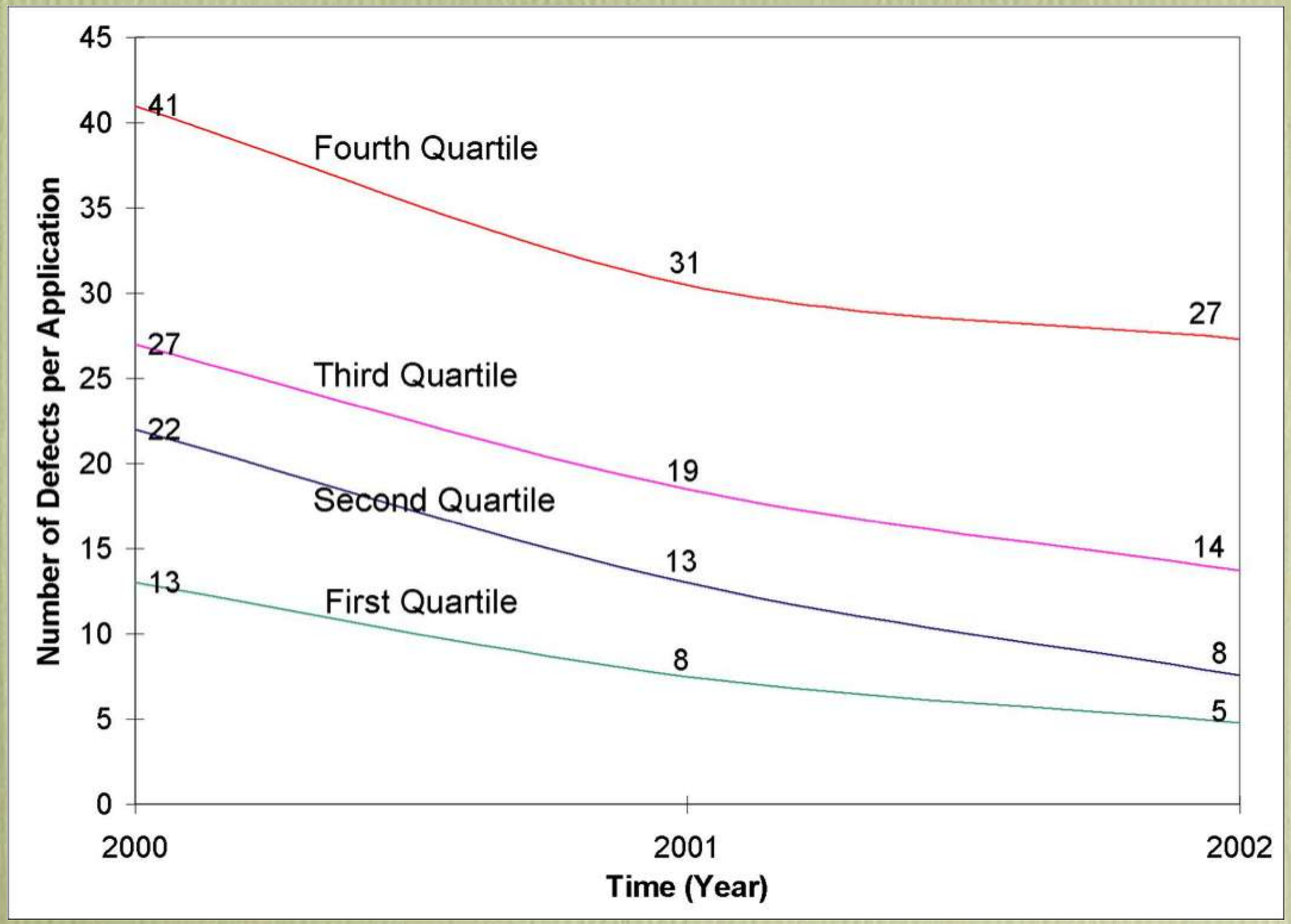
We need a common language

We need metrics for…

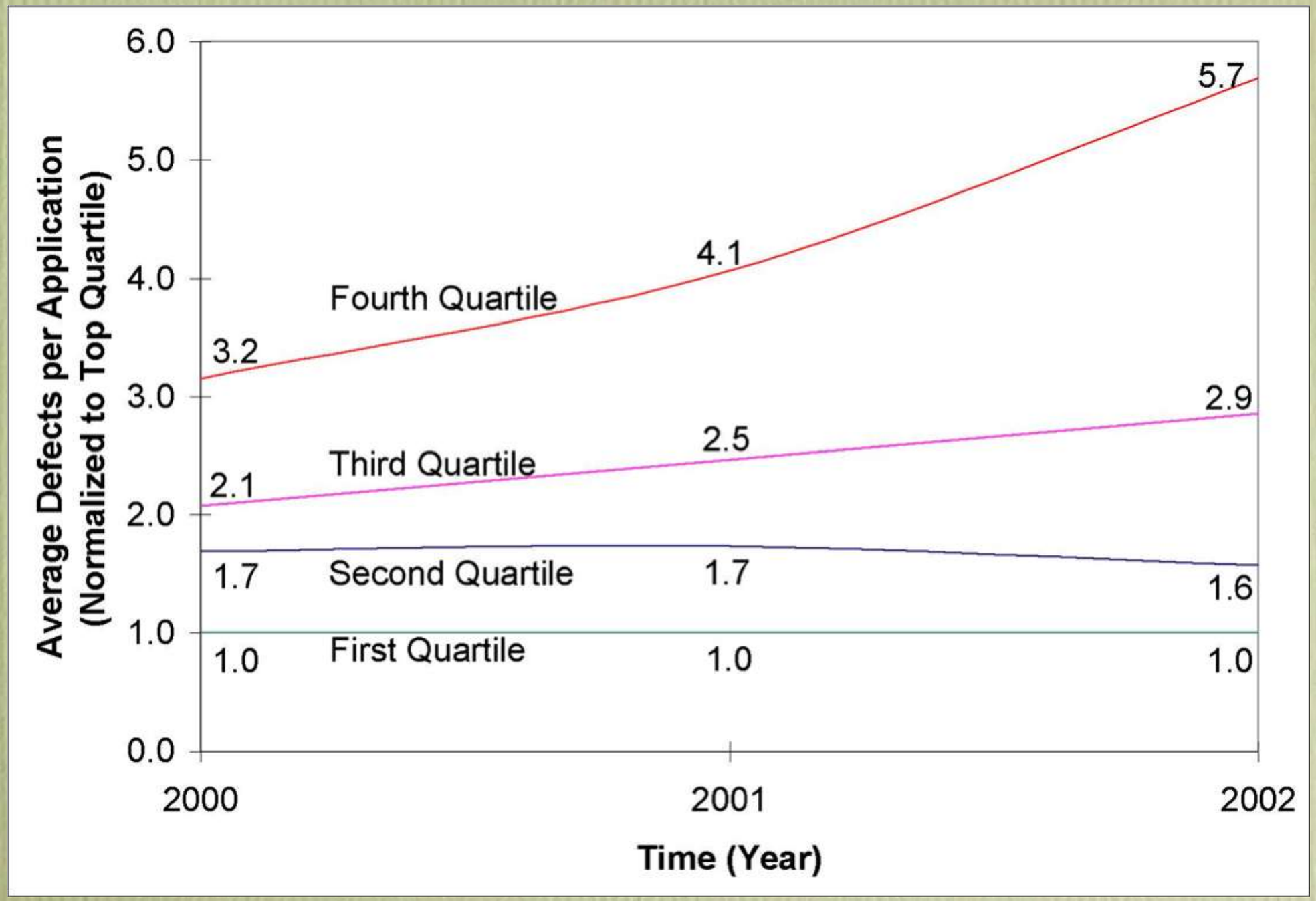
- How secure am I?
- Am I better off than I was this time last year?
- Am I spending the right amount of money?
- How do I compare to my peers?
- What risk transfer options do I have?

Some metrics already exist

Applications <u>are</u> improving



So counterparty risk rises



Meaning the security design goal for grids is what?

Accountability = design goal

- Cost(Access_Control) α { N(people) x N(functions) }
  - Grows faster than linear hence unscalable
- Accountability only alternative
  - Begs question of anomaly detection, not intrusion detection
  - Consistent with dissolved perimeter (inside≡outside)
  - Defers many costs to times of forensic necessity
- Selective data deletion more expensive that complete retention
  - cf. Privacy, limited discoverability

Grids as a security tool

- Target of choice *v.* target of chance
- Traffic analysis
- Forensic quality data cheap to retain
- Replication for reliability (hence security)
- Et cetera

The party has just begun

Summary

- Security is a subset of reliability
- Location independence is the focal point
- Economics ultimately rules
- Measurability by design is the only answer

Dan Geer
geer@stake.com
+1.617.768.2723