



ORACLE
FUSION MIDDLEWARE
IDENTITY MANAGEMENT

11^g

ORACLE[®]

Scaling Identity, Access, and Audit Controls To Internet Proportions

Mike Neuenschwander

A Modern Instance...

- Talking about scale in the Internet age: a good problem to have!



Questions of Scale

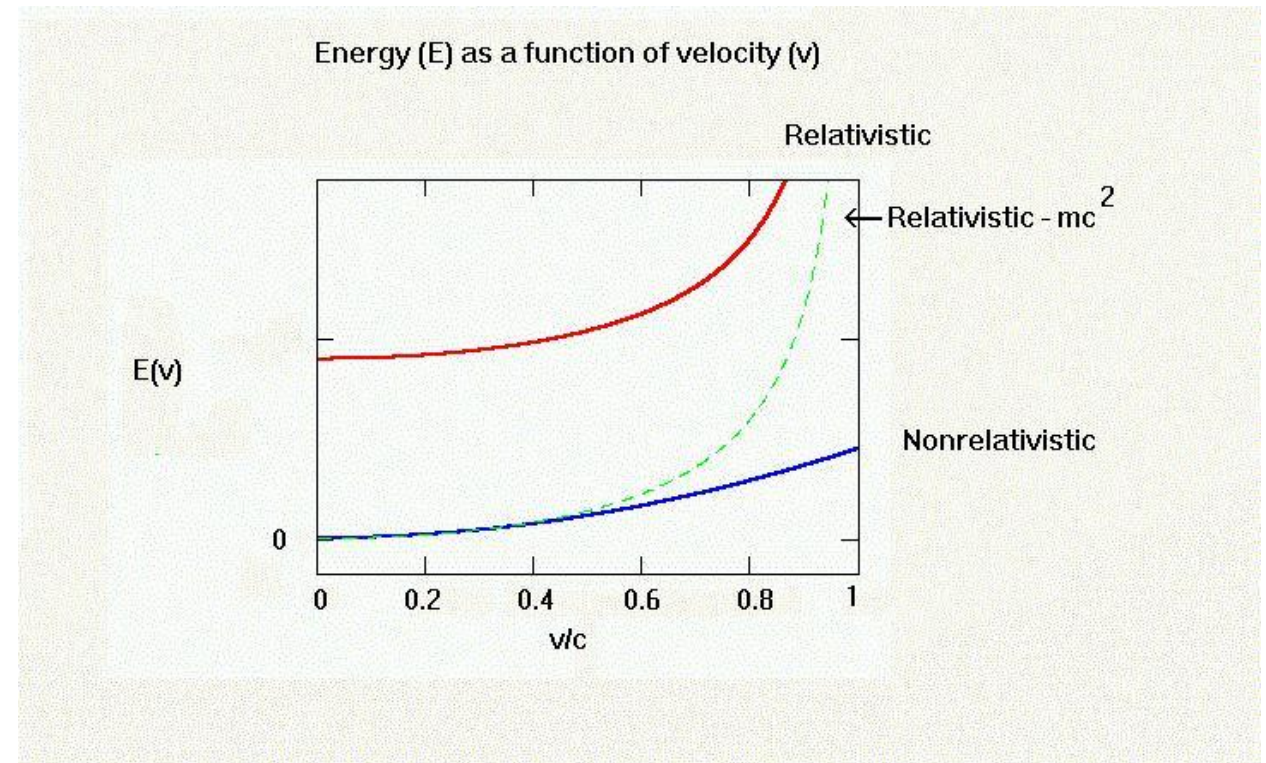
When the coefficient of management overhead can't be ignored

- How does an organization connect 70,000 partners in a year?
 - And maintain them?
- How can an organization manage 200 million users?
 - With a turn-over rate >20% annually?
- How much hardware is required to support 10 million entitlements?
 - And 1 million roles?
 - How can I provide auditors evidence of compliance at this scale?
- For Internet scale, how efficient do admins need to be?
 - How many admins are needed?
- **Bottom line: Today's I&AM tooling isn't up to the task**



Relativity & Scale

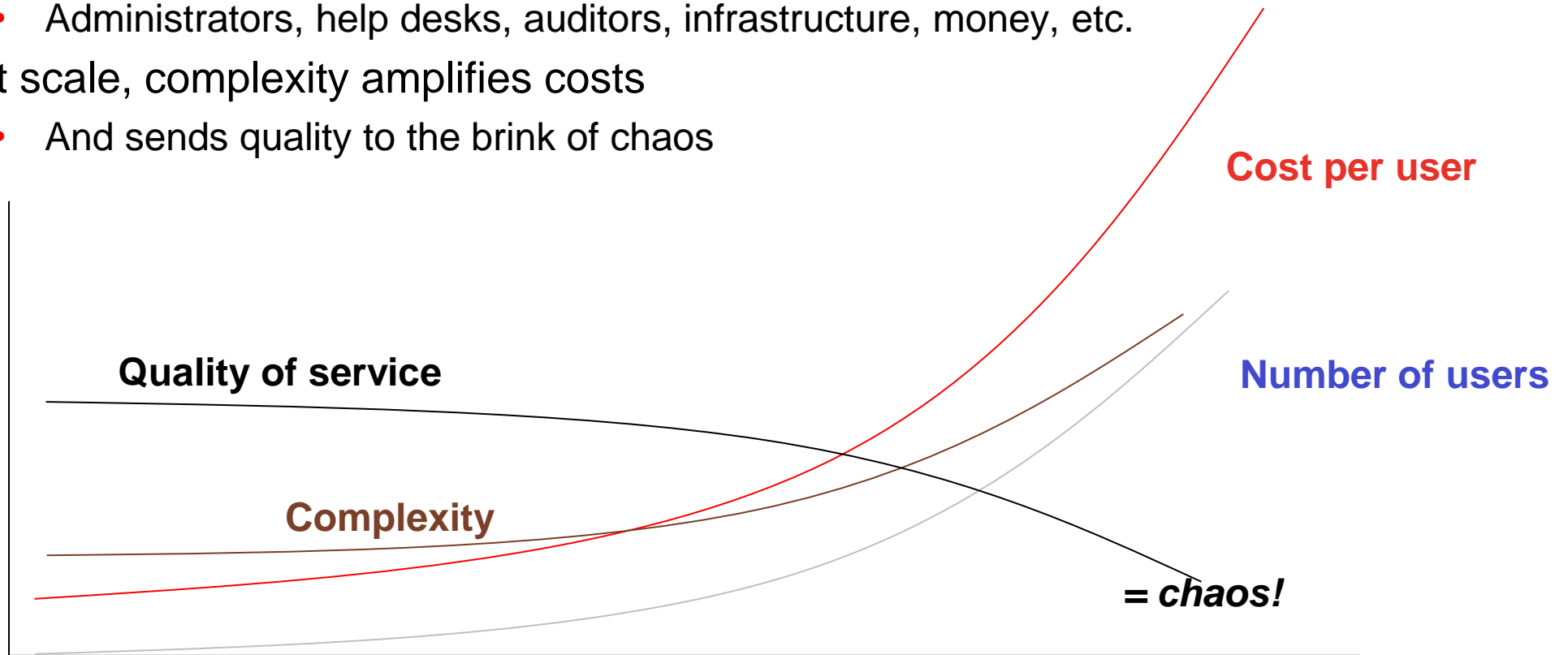
- Einstein's theory of Special Relativity
 - Showed how relativistic effects applied to objects at very high speeds
- Similar thinking is needed for scaling identity
 - Classical model breaks down at high scale



Relativistic Effects are Costly at High Scale

Cost model for identity management

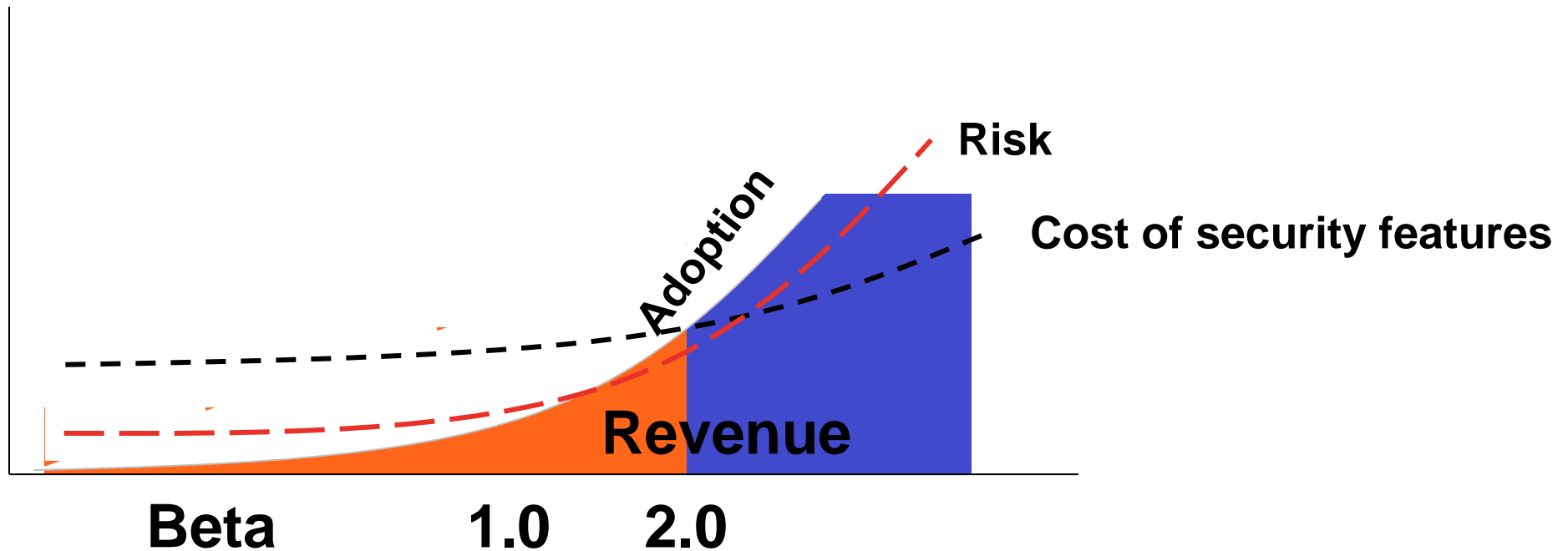
- Successful system = more users 😊
- But you'll need more resources, too ☹️
 - Administrators, help desks, auditors, infrastructure, money, etc.
- At scale, complexity amplifies costs
 - And sends quality to the brink of chaos



Relativistic Effects are Costly at High Scale

Software development is a function of user count, too

- Cost justification of administration, security, controls
 - Too expensive and constraining to build strong controls at beginning
 - Only go back to fix the system after it breaks
 - Which is the worst time to attempt fixing the problem



Relativistic Effects are Costly at High Scale

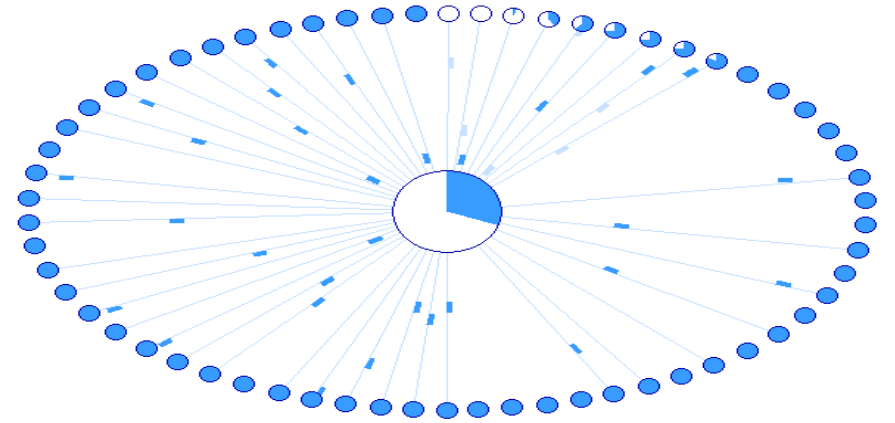
Can systems become more resilient and secure with scale?

- In dynamically resilient systems,
 - Each additional user introduces a net benefit (rather than a cost) to the system
 - Cohesion improves with the addition of each node
 - Resilience is built-in and scales from 10 users to billions of users



Relativistic Effects are Costly at High Scale

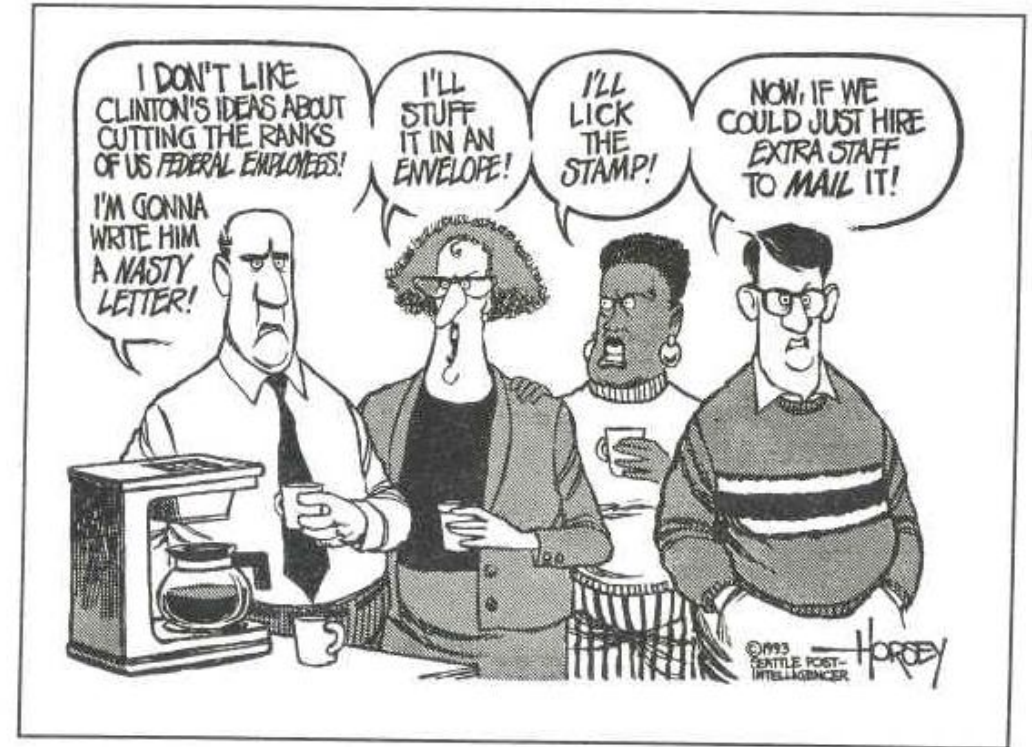
- Precedents for dynamically resilient systems
 - Examples include
 - BitTorrent
 - SETI@home
 - Social networks
 - E-mail
 - The WWW
- No perfect systems
 - No single system exhibits all characteristics of dynamic resilience
- *To meet high scale requirements, we need a new approach*



The Role of Administrator @ Internet Scale

- Enterprise I&AM market today
 - Focused on making administrators more efficient
 - That is to say, I&AM *enshrines the administrative role*
- Administrators should manage the infrastructure, not the population
 - Prevalence of administrators indicates something went wrong
- Ergo: *If adding users requires more admins, it's broke already!*

The Federal Bureaucracy



A Word on Chaotic Expansion

“As networks become more interconnected and complex, they simply cannot be centrally controlled.... In the case of the Net, it is designed to grow arbitrarily large and diverse because all of the **components are not dependent** on one another. Every **new user** or new device **does not have to have the permission** of other devices to be added to the network.”

— John Clippinger, *A Crowd of One*

Relying on Pro-Sociality

Appropriators are active participants in creating the dilemmas that they face, and under certain conditions, if given the opportunity, active participants in resolving them. They are not inevitably or hopelessly trapped in untenable situations from which only external agents can extricate them.

— Edella Schlager

from “Collective Cooperation in Common Pool Resources”

Security isn't always structural

Other forces at play

- Just because something can be stolen doesn't mean it will be
 - Mikey's law
- In defense of weak security
 - Maybe this security is sufficient for the society in which it's used
 - It's a place I'd like to live in!



Why isn't defection rampant?

Betrayal doesn't occur as much as it could

- What keeps people from “defecting” in relationships?
 - Locks and security systems?
 - Identification programs?
 - Police?
 - Contracts?
- These things can help, but don't entirely explain human behavior
 - They can also cause blowback

What forces bridle self-interest?

Why do bad things *not* happen when they easily could?

- Altruism and Brownian motion
 - You will see a multitude of tiny particles mingling in a multitude of ways... their dancing is an actual indication of underlying movements of matter that are hidden from our sight...
 - From Lucretius's *On the Nature of Things*
- Why are people altruistic?
 - Or at least social?
 - Or at least peaceful?
- Why do people cooperate?

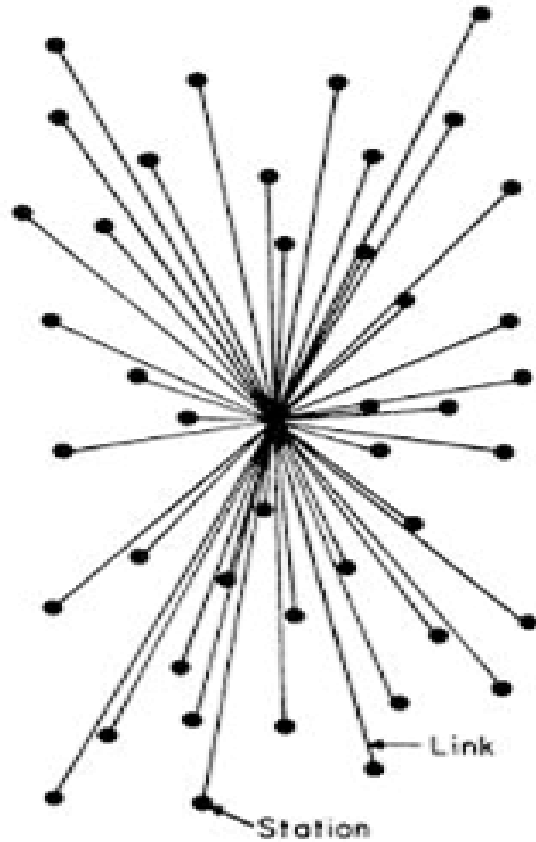


Let's agree to call it "trust"

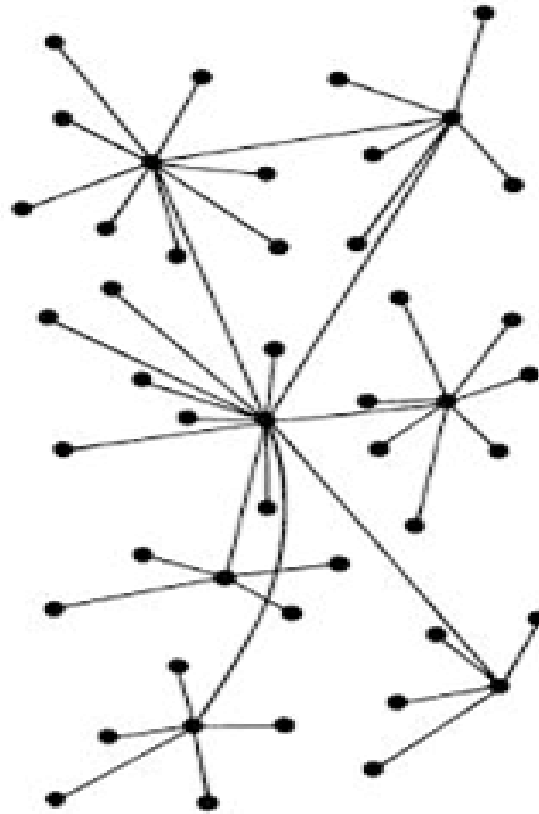
Short for "multilateral, durable collaborative action"

- Trust is not synonymous with hope
 - ... Or faith or belief
 - ... Or voodoo
 - ... Or touchy-feely
 - ... Or, for that matter, cryptographic algorithms
- A multilateral, durable collaborative action
 - A relationship in which participants are cooperatively working for a benefit, even when the roles, risks, and rewards differ
- If trust regulates defections in relations...
 - Can trust be cultivated?

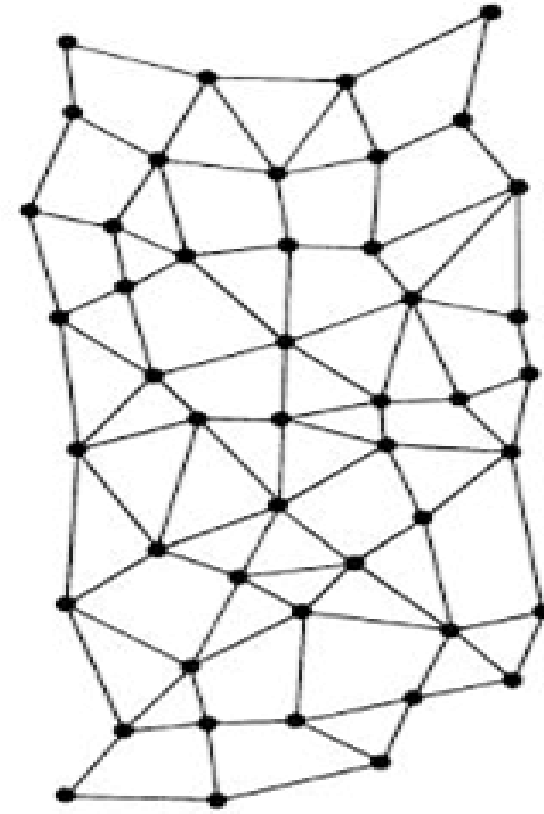
What Model Scales Best: Hub and spoke or mesh?



CENTRALIZED



DECENTRALIZED



DISTRIBUTED

Distrust **Trust**

Trust and Distrust: Not Polar Opposites

Approaches with vastly different methods

Distrustful	Trustful
Command-control	Roles and shared duties distributed among participants
Emphasis on security	Emphasis on transparency to parties
Dependency on a provider	Each party assesses the others' capabilities
1 big player (alpha player)	Distributed roles and responsibilities
Explicit contracts, frequent checkpoints, vigilance	Transparency among participants
Broad swath	Fine grained and nuanced
Hierarchical	Matrixed
Formal	Informal
Regulation	Informal rules, agreements
Coercion	Cooperation
Structural solutions	Collaborative solutions

Instruments of Cooperation

The tools in use affect the relationship

Tools of *distrust*

- Identification card, identity assurance, encryption, rights, management, access control, policy



Tools of *trust*

- Reputation, reciprocity, empathy, signaling, collaborative action, recognition, shared experience, social interactions, ceremony, connection



Interaction of Trust and Distrust

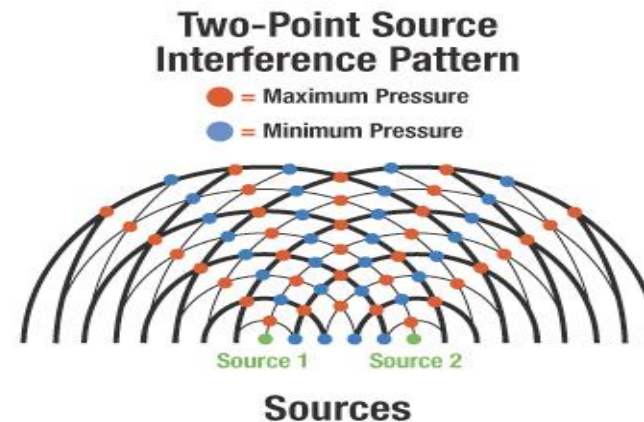
Harmonic Resonance and Interference

- Resonance

- A system of distrust may improve systems of trust when
 - It defines a boundary within which laws are enforced
 - It systematically defines process for arbitration

- Interference

- A system of distrust may interfere with trust when
 - It cultivates an environment of suspicion and negative social emotions



Can Trust be Trusted?

While not always feasible, the trustful model is stable

- Highly trustful relationships
 - Are inherently more resilient and secure than distrustful relationships
 - Are better at problem solving than distrustful relationships
- Nevertheless, *our industry is over-invested in distrust*
 - Which makes us look a bit funny



A theory of trust

Principles for cultivating trust



- Elinor Ostrom observed that governance of a shared resource is sustainable if the following design principles are adhered to:
 - **Exclusion** – The group must be able to guard the resource from free loading, theft, or vandalism.
 - **Rationality** – The agreed upon rules must be attuned to the context of the resource
 - **Involvement** – Members have avenues to participate in modifying operational rules
 - **Monitoring** – Effective monitoring and auditing or policies
 - **Enforcement** – Sanctions can be imposed on violators of the rules
 - **Arbitration** – Appropriators have access to low cost, but effective conflict resolution
 - **Autonomy** – The rights of appropriators to devise their own institutions are not challenged by external governmental authorities

The Proposal: Trust as a Protocol

Rules of engagement for the modern era

- The new Trust Anchor: “Trust Protocol”
 - Don’t need to trust the other party (human or not)
 - Just need to reliably believe that if you conduct your relationship according to the trust protocol, you’re less likely to get screwed over
 - The role of the trust protocol is to promote collaborative outcomes
 - Incentives to cooperate
 - Demonstrably lower defection rates compared with distrust & no-trust models
 - Not just out-of-band documents, agreements, standards, and specifications
 - Built right into the very fabric of the Internet
- The new Actors: Personas
 - **All** actors are personas,
 - NOT natural persons, companies, governments, viruses, or malware
 - Personas must be registered

References

- Sources to find other sources
 - My blogs (past and current)
 - <http://hybridvigor.org/author/mike/>
 - identityblog.burtongroup.com
 - <https://blogs.oracle.com/OracleIDM/>
 - My reports & presentations
 - <http://www.cloudidentitysummit.com/Presentations-2010.cfm>
- Bruce Schneier's new book
 - Liars & Outliers: Enabling the Trust that Society Needs to Thrive