Four Perspectives on Risk and Trust in Cloud Computing

Carlos Trigoso
2010

Following the development of Cloud Computing, we can see two major trends arising: I&AM “for” the Cloud, and I&AM “in” the Cloud; essentially security services to protect the Cloud (hosted) environments, and security services offered by remote shared platforms. The two are inseparable …

We have adopted the terms of Security “for” and “in” the Cloud to reflect two “views” we find among clients and specialists

Security for the Cloud: Securing the broader IT application and data workloads as they migrate from corporate data centres into Cloud services

Security in the Cloud: Cloud as a delivery model for security service providers – for example identity management as a service, or compliance as a service

Different perspectives and different actors

Security for the Cloud means the Objective position, the position of the implementer, the controller, the auditor, but also that of the engineer, the technologist, the IT organisations

Security in the Cloud, points to the Subjective position, the position of the business leader, the owner, the strategist, but also that of the group, the organisation, Society at large

There is an ongoing, continuous widening of the range of user types. Is there no „internal“ space anymore?

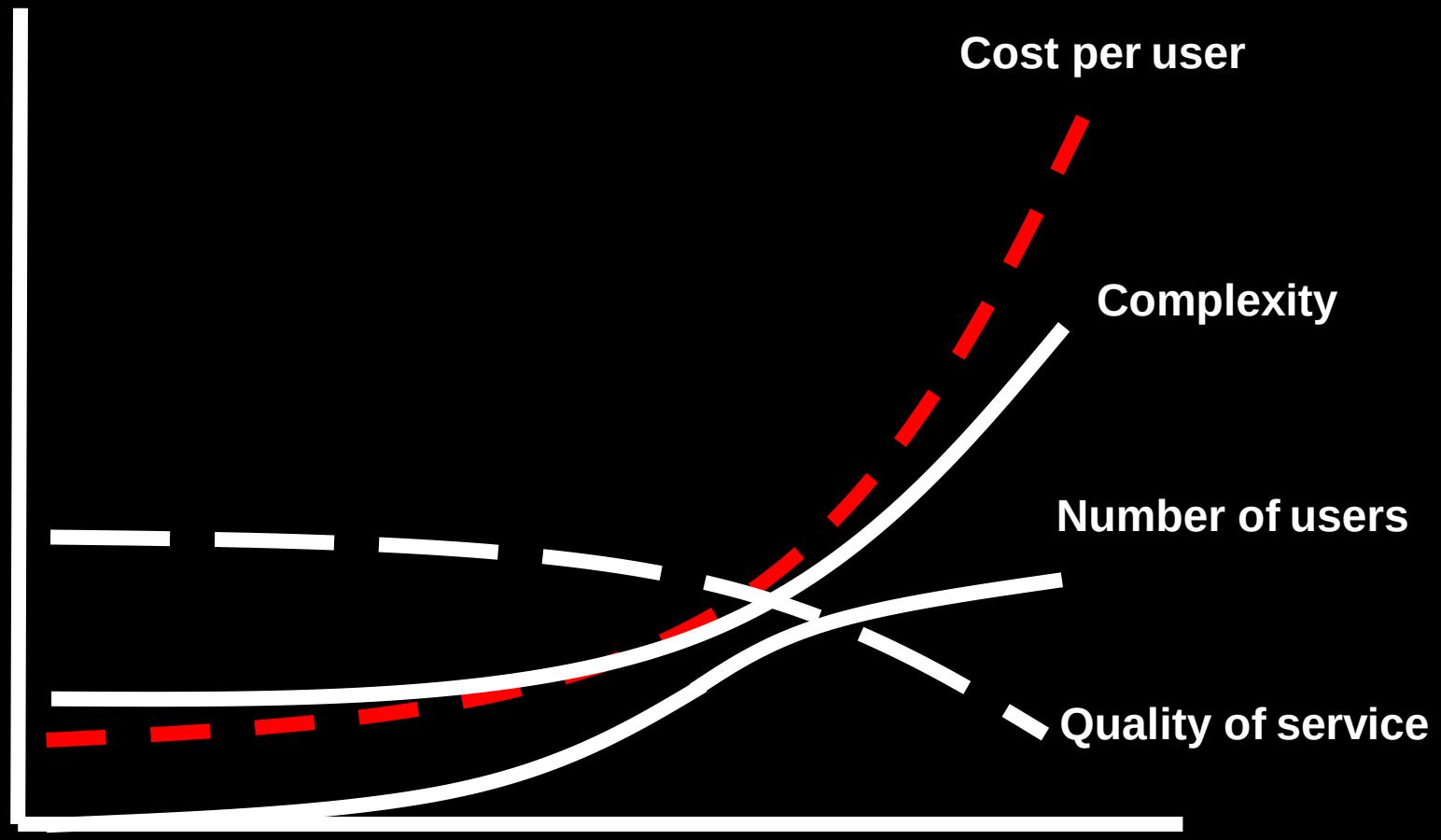
A fundamental change: the variety of users increases and the range of valid access rights blurs the distinction between internal and external realms

To address these challenges, technology vendors and practitioners adopt naturally different perspectives, world-views which inevitably impact the nature of the proposed solutions

In the model here proposed, there are four disciplines or “perspectives” integral to Security: Direction, Selection, Protection and Verification

Cloud Adoption: Complexity and Security costs limit adoption

(according to M. Neuenschwander)



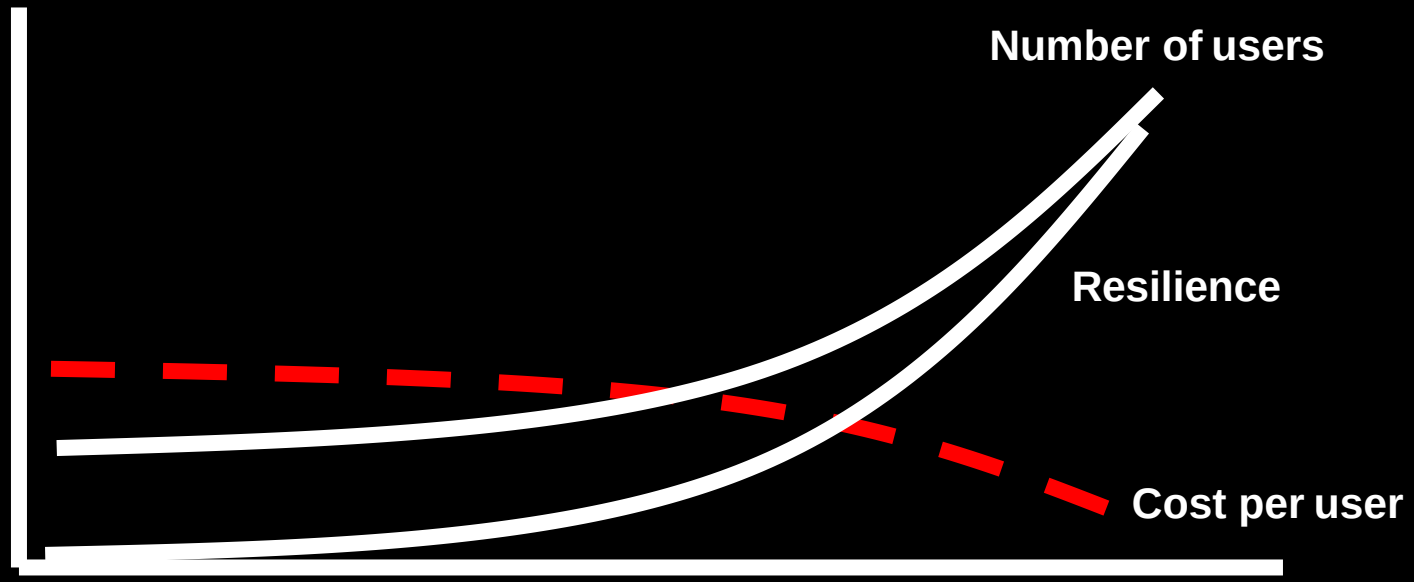
Is there a ceiling for Cloud adoption?

We see persistent doubts and demands for increased assurances in terms of data protection, cross-border operations, data ownership and processing, out-sourced operations and service provisioning

The subjects of Risk and Trust appear frequently contra-posed, in discussions about Security for and in the Cloud; but also in relation to the Business Organisation

Cloud adoption seems to be hampered by issues of Risk and Trust, both on the side of the Enterprise and that of the Consumer

Increased resiliency and shared capabilities should result in significant cost reductions.
Success = more users?



Risk and Trust: Contradictory, Contrary or Complementary?

The view of Security as anchored on Risk Management has dominated our profession

The key is though, that there is no Trust without Risk, that these concepts are interdependent and correlated

Trust involves Risk, Risk involves Trust

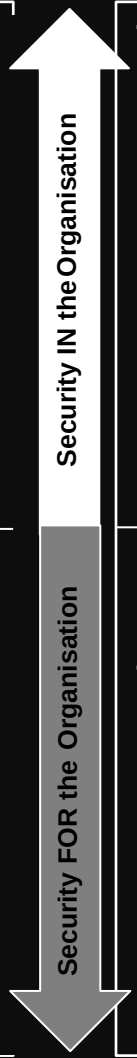
Trust Management Centred View

Trust Definition

In this space, Security is seen from the perspectives of Direction (Trust Definition)
Identity is seen as Distinction

Trust Allocation

In this space, Security is seen from the perspective of Selection (Trust Allocation)
Identity is seen as Membership



Trust Verification

In this space Security is seen from the perspective of Detection (Trust Validation)
Identity is seen as Context

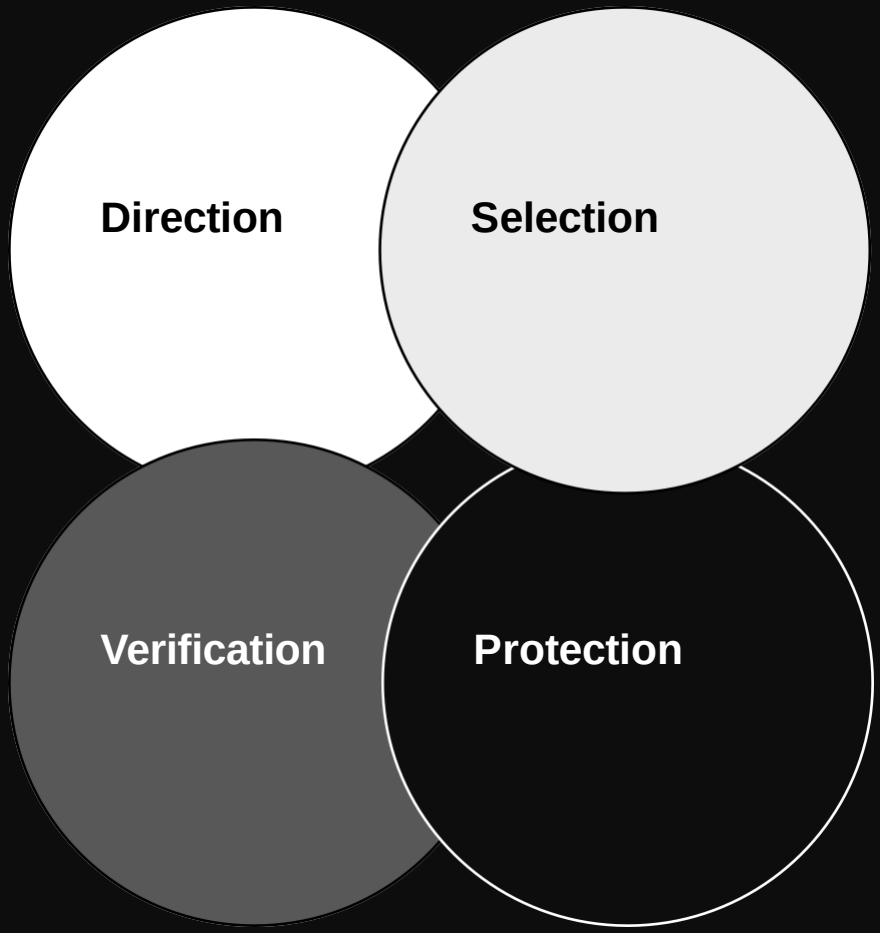
Trust Enforcement

In this space Security is seen from the perspective of Protection (Trust Enforcement)
Identity is seen as Object

Risk Management Centred View

The Four Security Perspectives

DIRECT:
Business Strategy
Define Trust /Collaboration
Manage Business Operations
Governance (Decision Making)

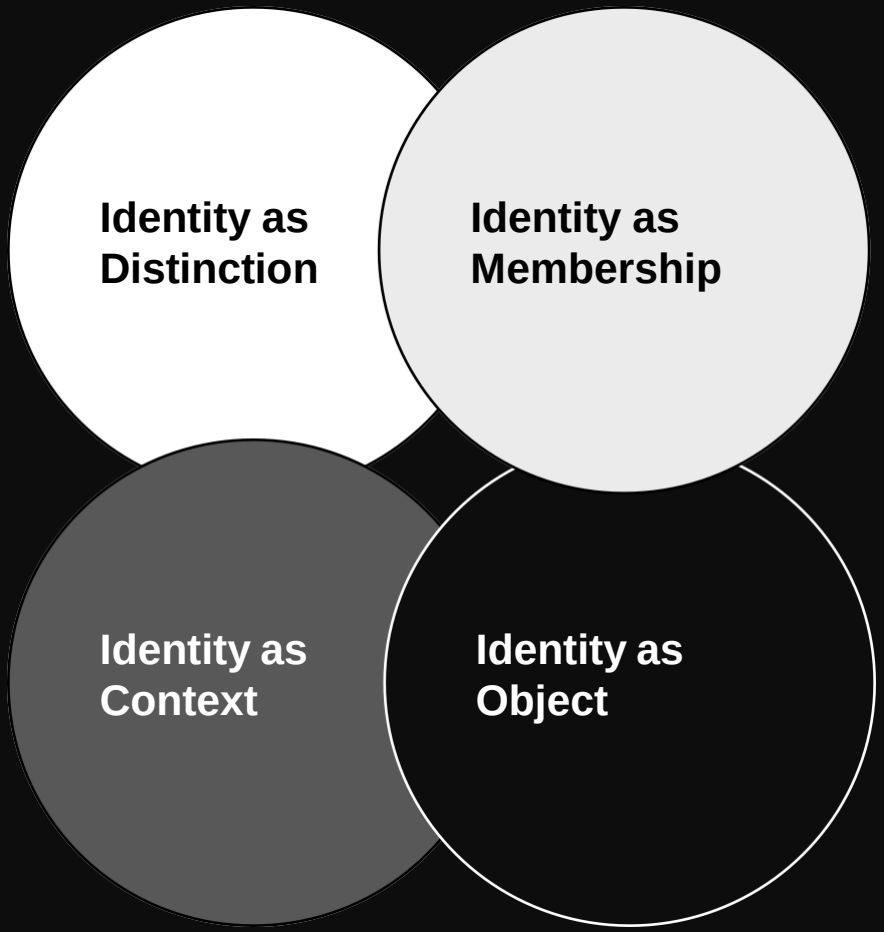


SELECT:
Organisational Model
Establish Trust /Collaboration
Manage Authorisations/Roles
Confidentiality

VERIFY:
Business Control Functions
Verify Trust/Collaboration
Manage Compliance/Audit
Integrity

PROTECT:
IT Security Controls
Enforce Trust
Manage Perimeter/Access
Availability

The Four Security Perspectives: Fundamental Identity Concepts



Minds, Organisms, Machines and Templates: Four System Metaphors

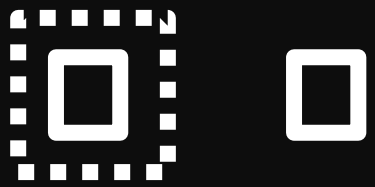
(according to R. Jung)

The most frequent form of architectural diagrams is a composite of arrows and boxes, “objects” we define, and their relationships
The class of relationships reveals the systemic metaphor in use:

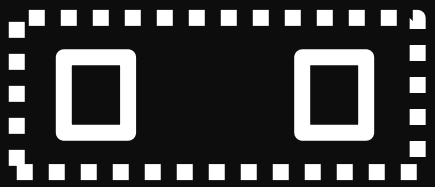
- Systemic action as distinction (value)
- Systemic action as membership (relationship)
- Systemic action as object (flow)
- Systemic action as context (protocol)

The Four System Metaphors

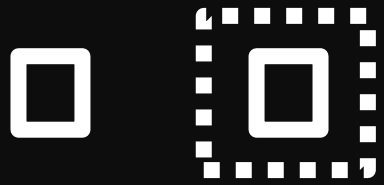
MIND: Systemic action as distinction



ORGANISM: Systemic action as membership



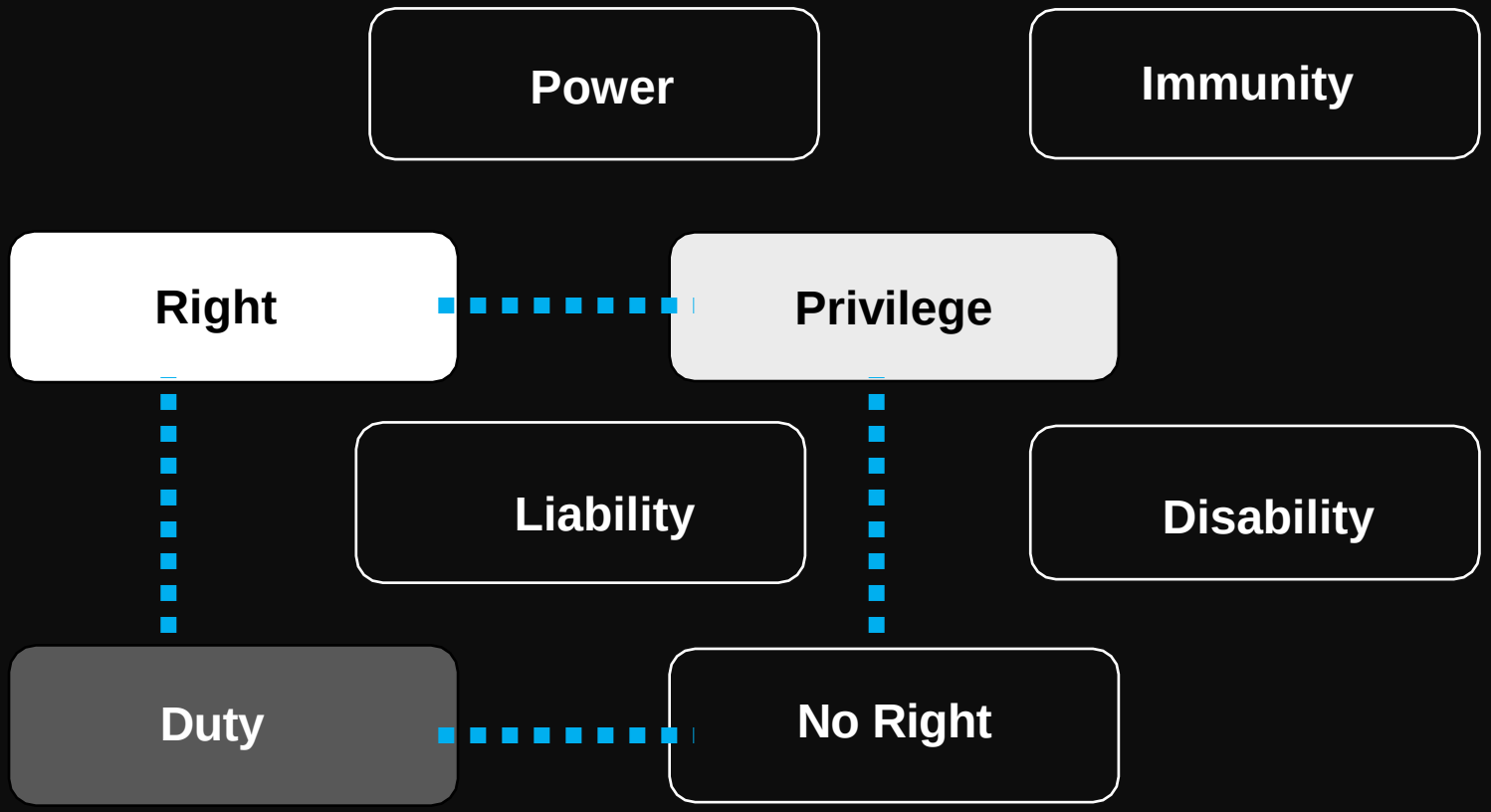
TEMPLATE: Systemic action as context



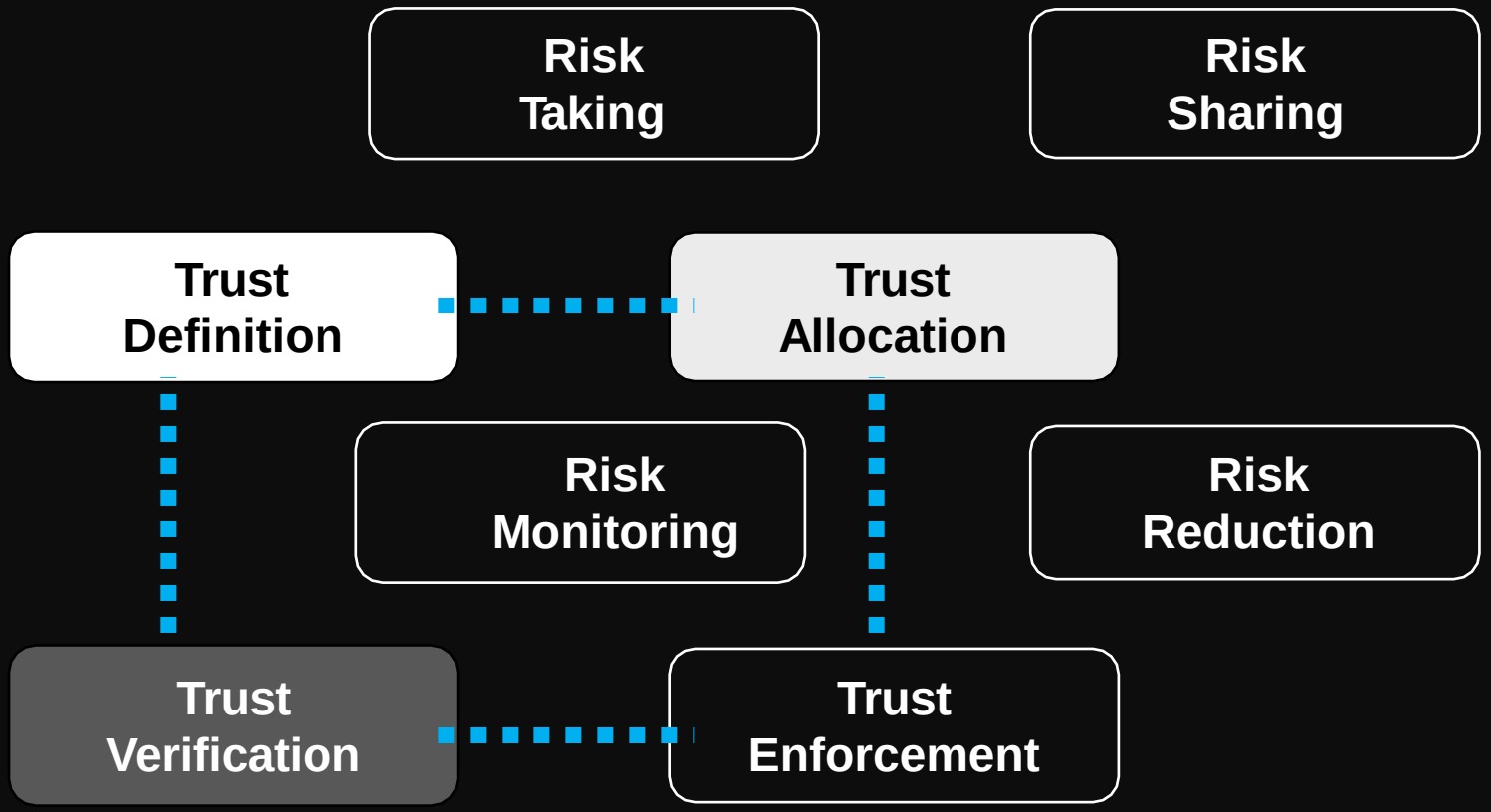
MACHINE: Systemic action as object

The Jural Opposites and Correlatives

(according to W. N. Hohfeld)

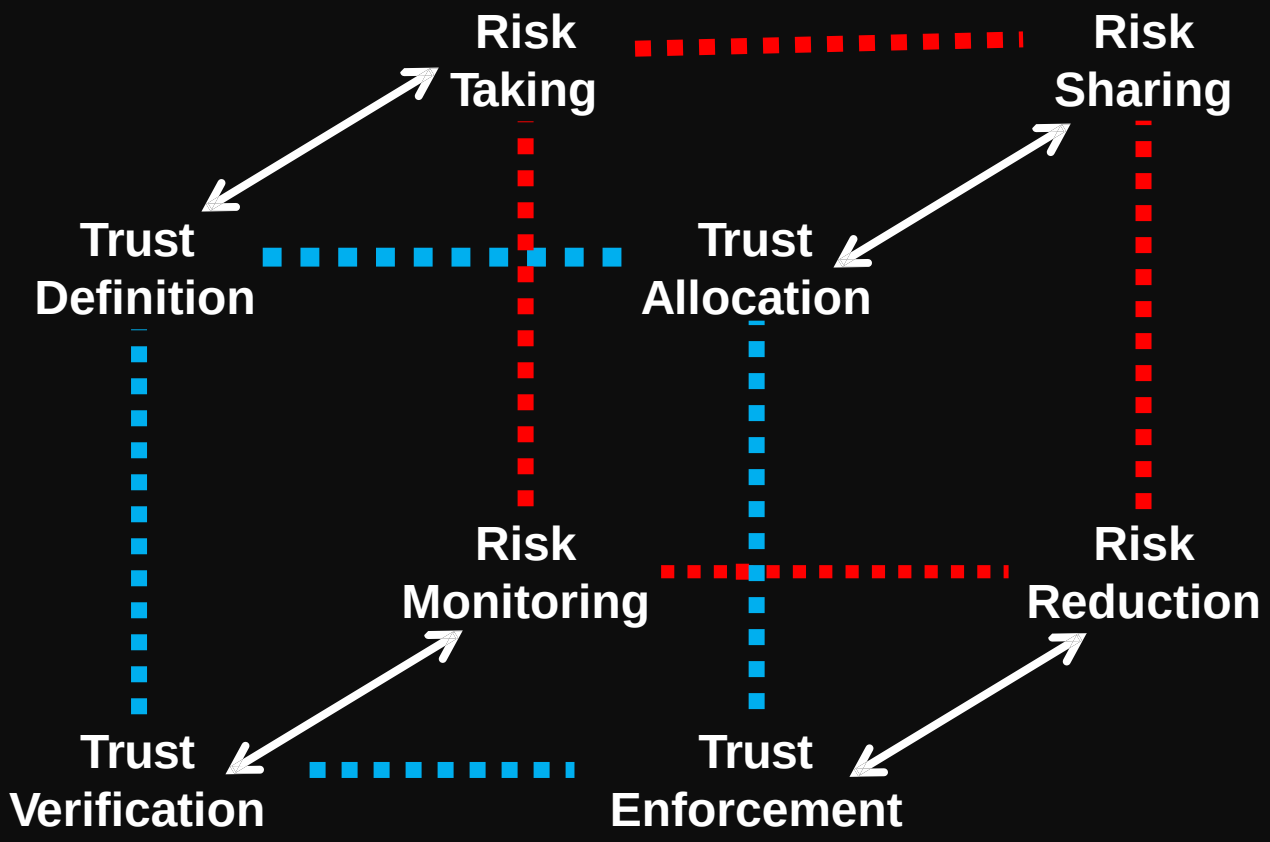


The Fundamental Security Perspectives



Trust involves Risk

Risk and Trust are co-dependent concepts, in a wider Security conceptual framework.



Security for and in the Cloud / for and in the Organisation

The delivery of security for the Cloud is a correlate for the realisation of security in the Cloud: adoption of advanced Cloud services depends on this.

The view focused on security “for” the Cloud requires primarily assurances to adopt technology-based solutions

The view focused on security “in” the Cloud reflects the target state of any Cloud initiative: security as a service “in” the Cloud; a state where the primary concern is the variety of identities, not of technologies

Conclusions

The Risk-centred “view” predominates when deciding how to adopt Cloud-based strategies, the Trust-centred “view” predominates when delivering and exploiting Cloud-based services, but the two views are part of the same big picture and have to be mastered in the Cloud Security Strategy

In general it is advisable to keep in mind that the disciplines of Trust Definition and Allocation are still not well developed and tend to stay in the background. In the new world of Cloud Computing, nevertheless, it is essential to develop a balance between these disciplines and the more conventional and developed perspectives of Trust Enforcement and Verification

References

Donn B. Parker, *Making the Case for Replacing Risk-Based Security, 2006*

John Arnold, *Security Services Model – Security Architectures for the Modern Enterprise , 2006*

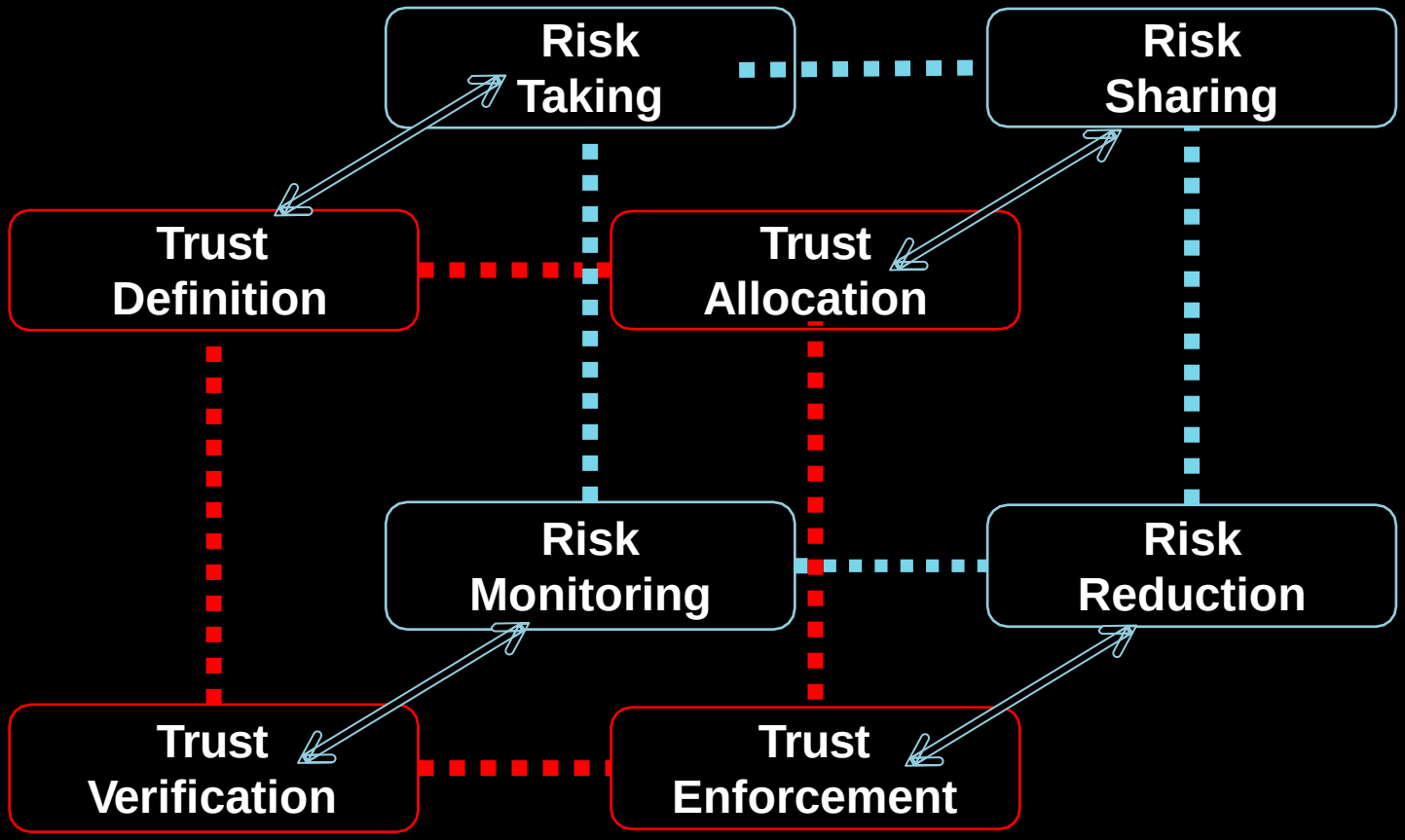
Hans Wierenga, *Why the Information Security Consultancy Industry Needs a Major Overhaul, 2010*

Mike Neuenschwander, *Thinking Outside the Domain - The Emergence of User-Centric Identity and the Trend Toward Pro-Social Management Systems, 2006*

W.N. Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning, 1913*

Richard Jung, *A Quaternion of Metaphors for the Hermeneutics of Life, 1985*

Niklas Luhmann, *Familiarity, Confidence, Trust: Problems and Alternatives, 2000*


Risk
Taking
Risk
Sharing
Trust
Definition
Trust
Allocation
Risk
Monitoring
Risk
Reduction
Trust
Verification
Trust
Enforcement