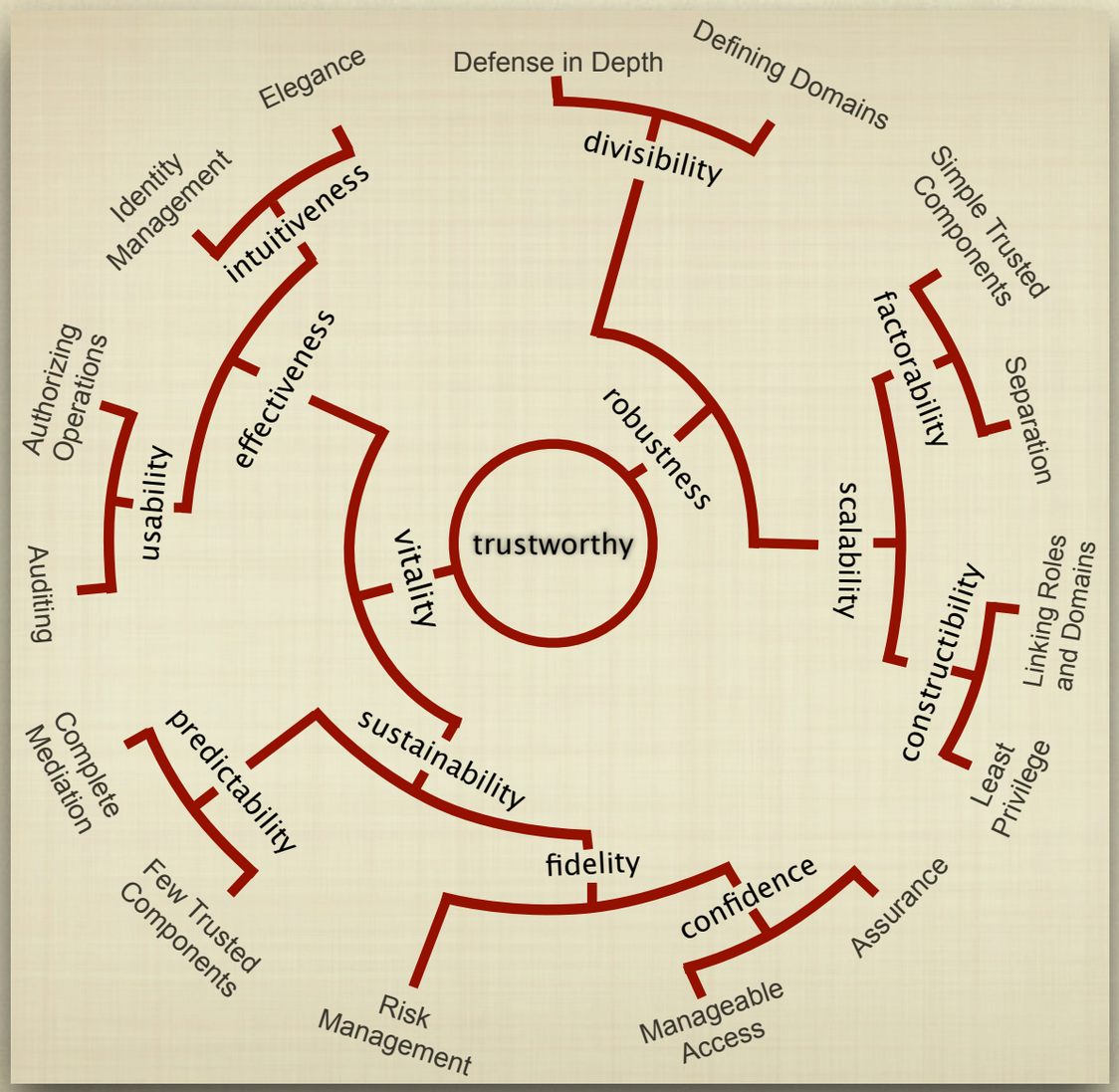
Towards a Design Theory for Trustworthy Information Systems



Les Waguespack, Ph.D., Professor

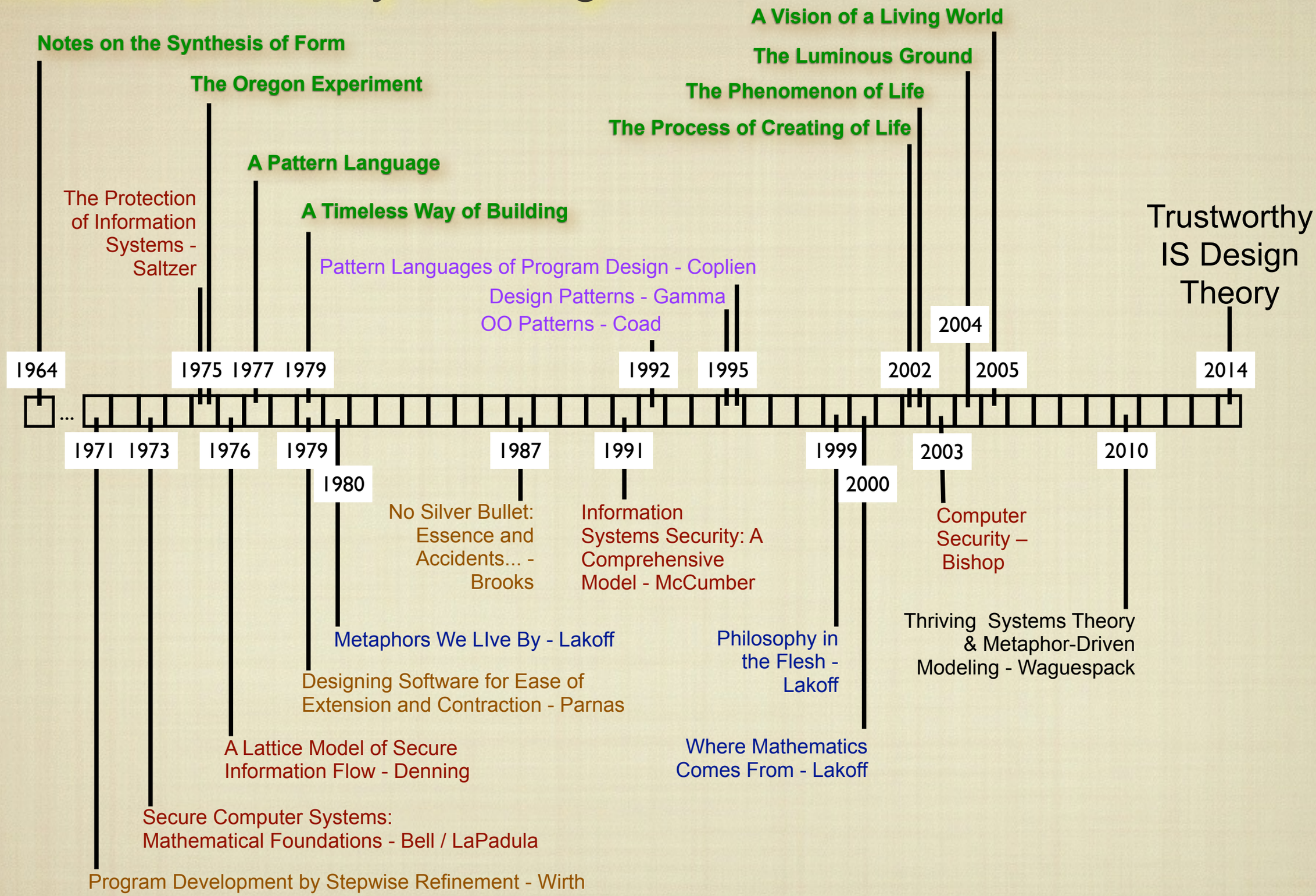
David J. Yates, Ph.D., Associate Professor

William T. Schiano, DBA, Professor

Computer Information Systems
Bentley University
Waltham Massachusetts

HICSS-47 - Hawaii
January 9, 2014

Threads of Theory in Design



Motivation

- The current state of design thinking about security has led to many gaps in information systems security.

Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Organisation for Economic Co-operation and Development (2002)):

A *"growing number and wider variety of threats and vulnerabilities"* marks the Internet Age.

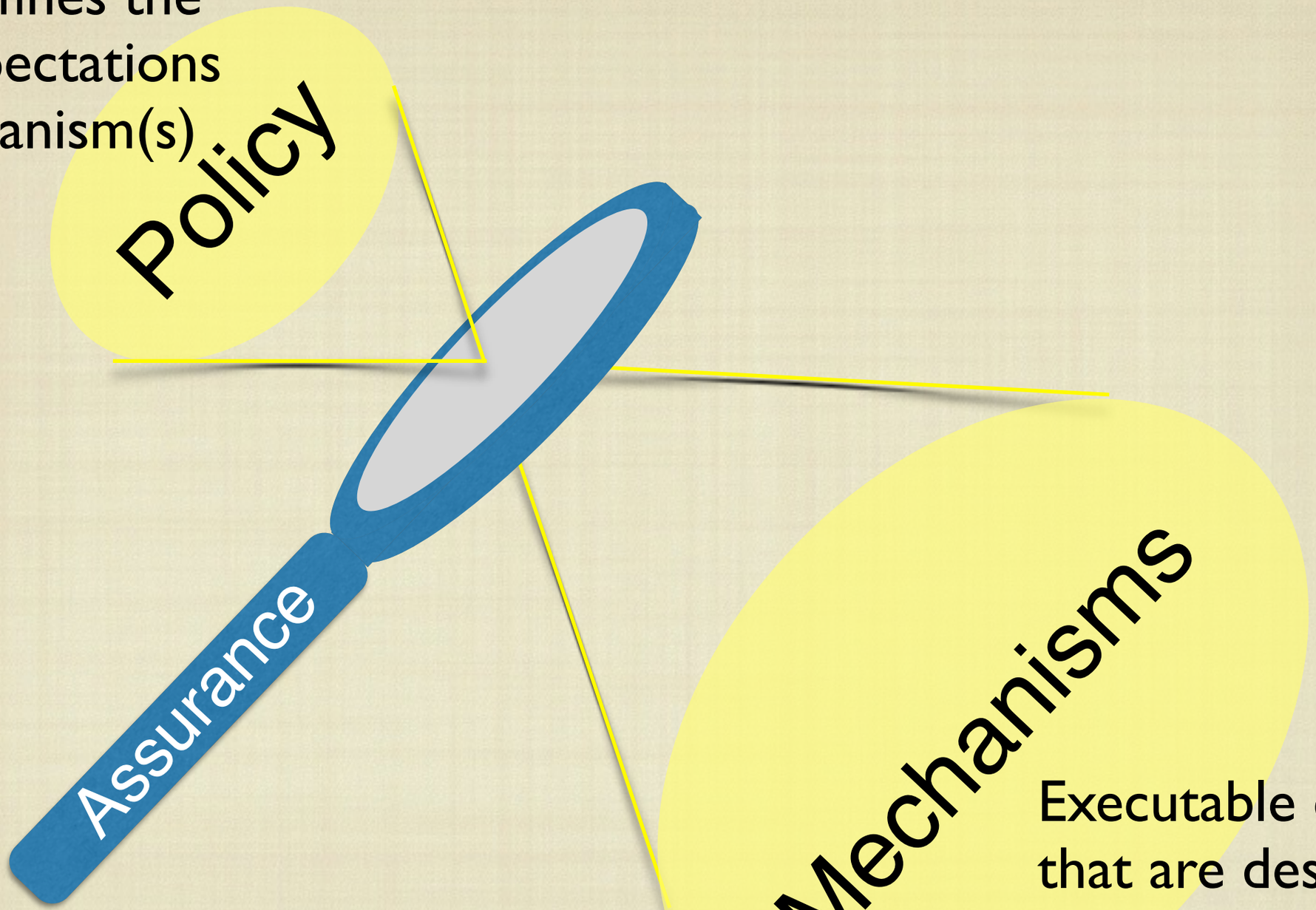
"Only an approach that takes due account of the interests of all participants, and the nature of the systems, networks, and related services, can provide effective security."

- We need a design theory for information systems and business models with principles of form and function:

1) that enable stakeholders to integrate the broad range of security concerns and potential responses,
2) in a balance that satisfies stakeholders' objective and aesthetic conception of quality and trustworthiness.

Assurance Engenders Trust

Statement of requirements that explicitly defines the security expectations of the mechanism(s)



Executable entities that are designed and implemented to meet the requirements of the policy

Assurance Engenders Trust

Statement of requirements that explicitly defines the security expectations of the mechanism(s)

Policy

Provides justification that the mechanism meets policy through assurance evidence and approvals based on evidence

Assurance

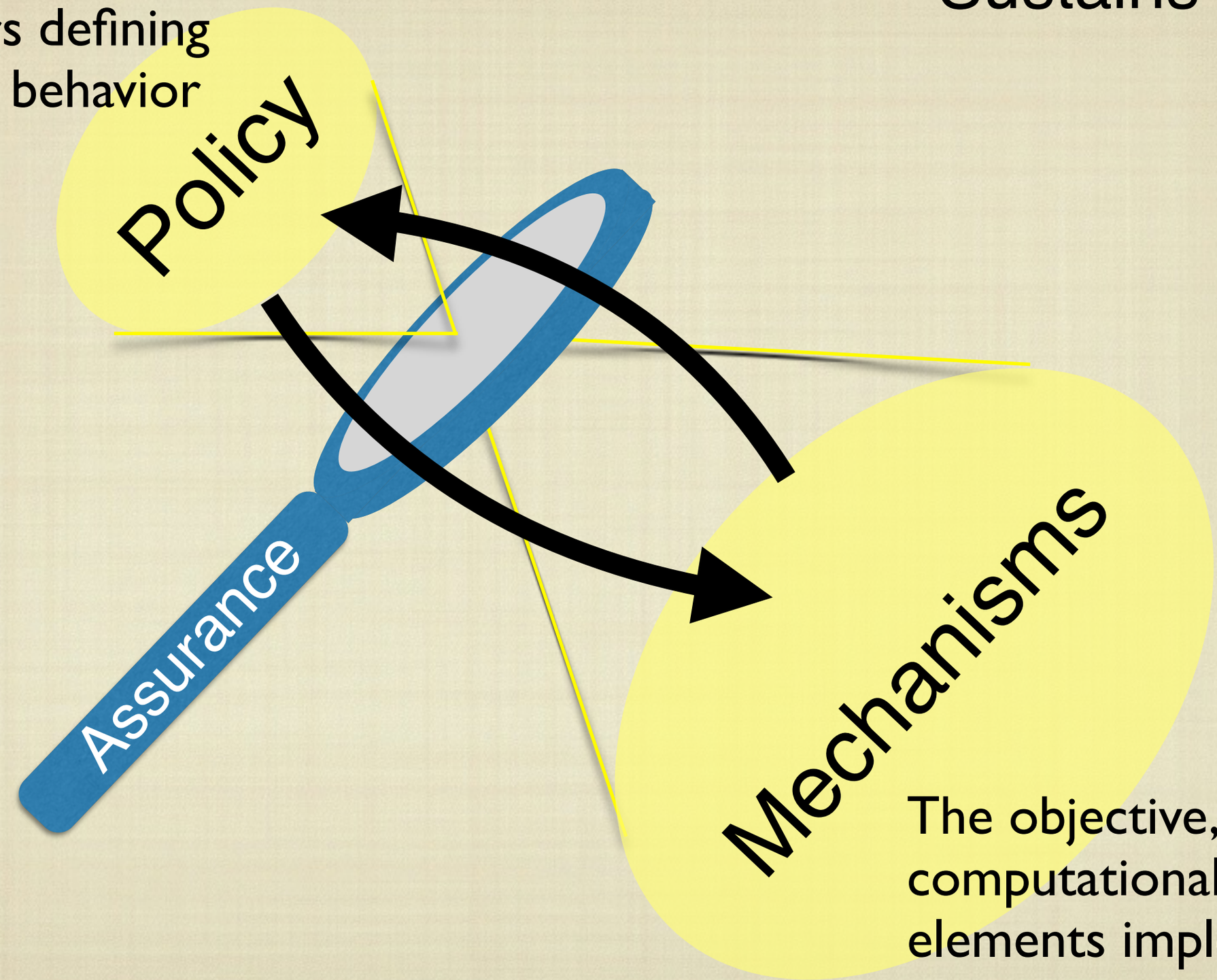
Mechanisms

Executable entities that are designed and implemented to meet the requirements of the policy

Bishop, p. 479

Security Management Sustains Trust

The subjective, intention of the stakeholders defining satisfactory behavior



The objective, computational elements implementing the "physical" security model

Security Management Sustains Trust

The subjective, intention of the stakeholders defining satisfactory behavior

Policy

A dynamic alignment of policy and mechanisms responding to emerging threats and evolving requirements: environment and technology

Assurance

Mechanisms

The objective, computational elements implementing the "physical" security model

Trustworthy Systems

"Security policies are assumed to be internally consistent and to reflect the requirements of the organization to which they apply. Similarly, security mechanisms are assumed to work correctly and to perform the functions for which they are intended. These crucial aspects of trustworthiness are commonly glossed over because they are difficult to quantify or analyze."

Elisabeth Sullivan

Part 6, (Bishop (2002), Computer Security: Art and Science, Addison-Wesley, Boston, MA.)

Trust in information systems must be driven by a combination of:

1) responding to the stakeholders' tacit expectations and
2) shaping those expectations by crafting a security model that defines trustworthy systems behaviors and outcomes.

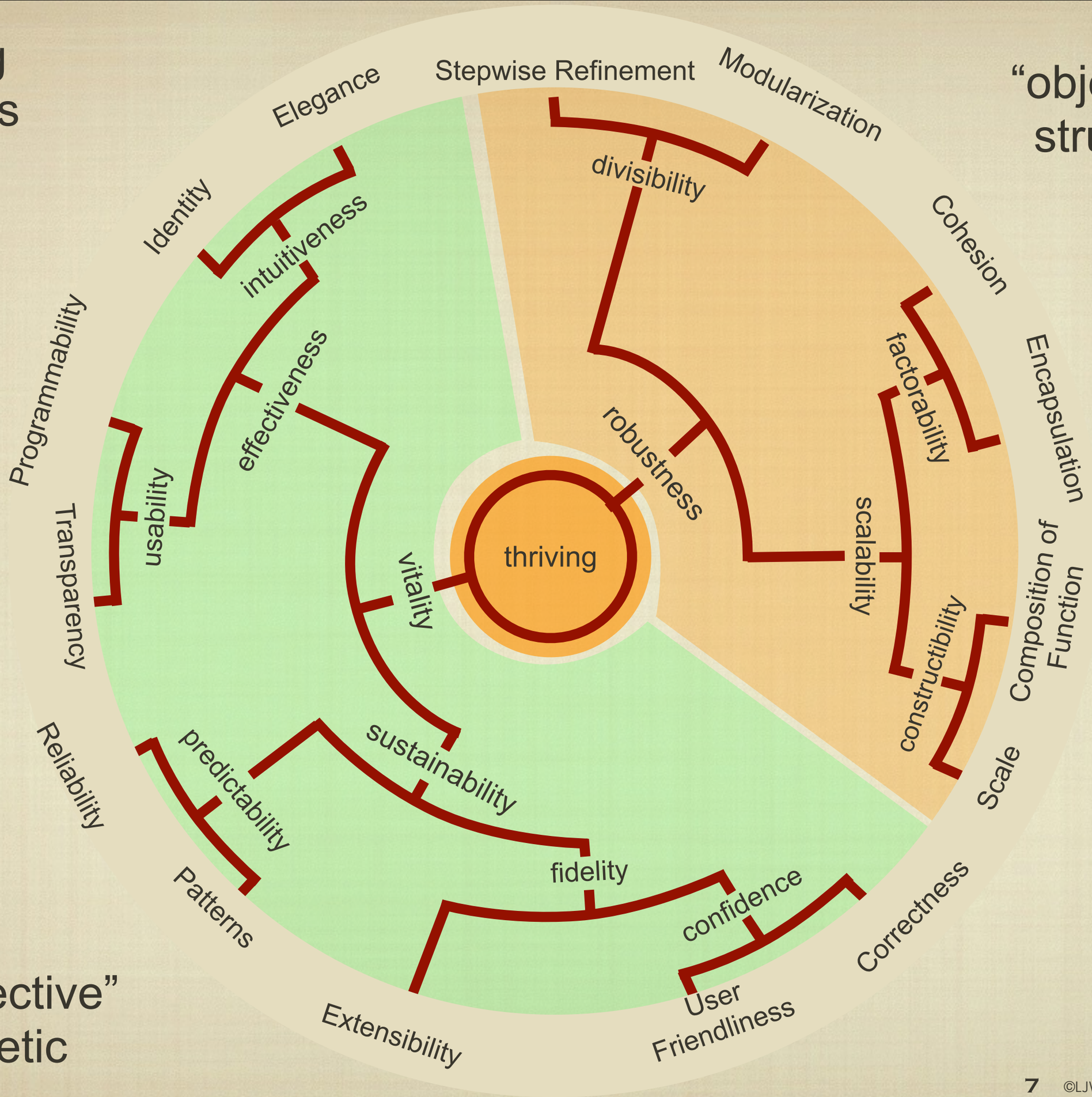
Thriving Systems Theory

Design Choice Properties in Confluence Experienced as Design Quality

Elegance
Stepwise Refinement
Modularization
Cohesion
Encapsulation
Composition of Function
Scale
Correctness
User Friendliness
Extensibility
Patterns
Reliability
Transparency
Programmability
Identity

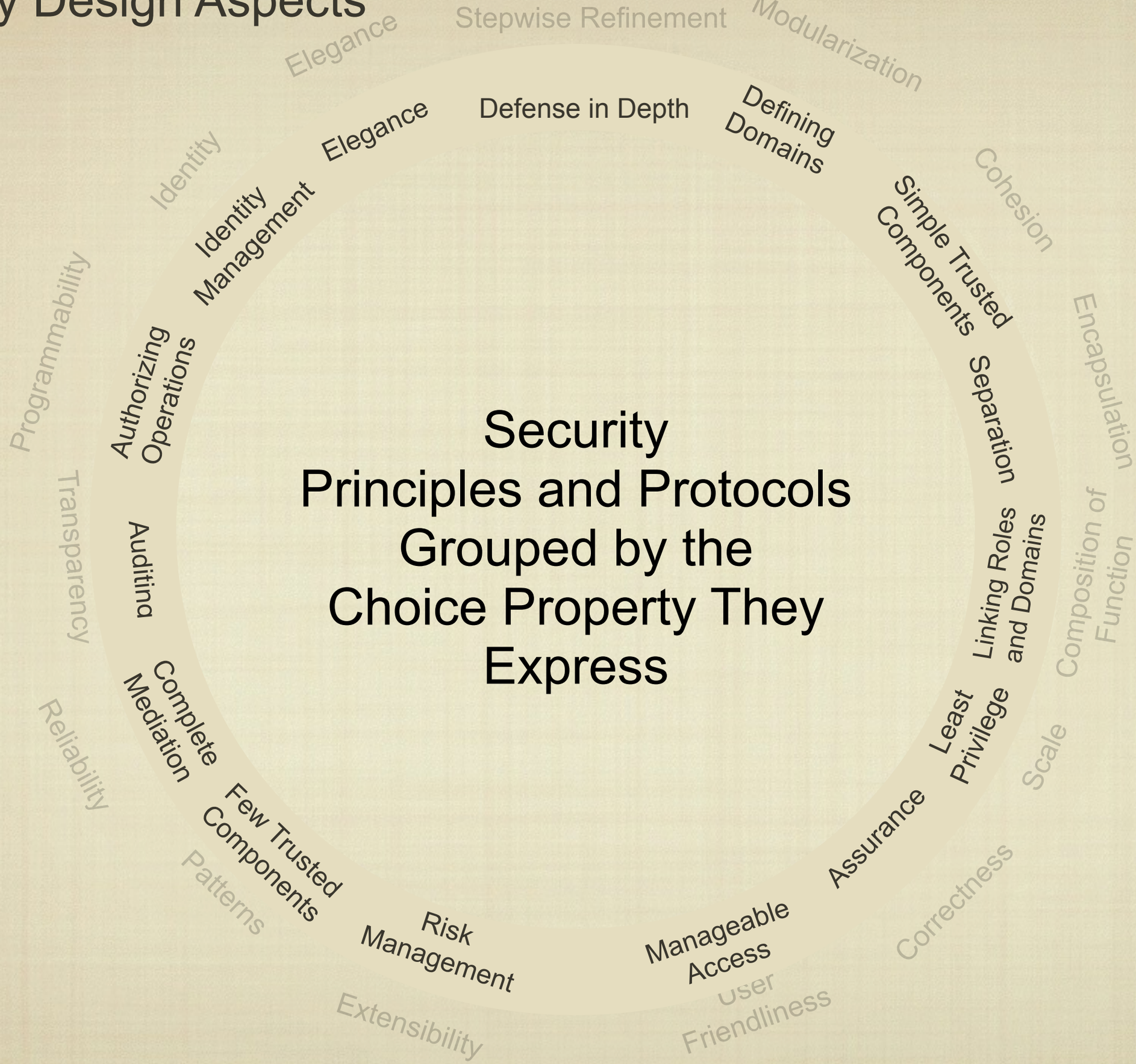
Thriving Systems Theory

"objective"
structural



"subjective"
aesthetic

Security Design Aspects



Security Design Aspects

Elegance: protection mechanisms effectively, efficiently, and simply organized, realizing a security policy resonating with the stakeholder community's conception of security and welfare

Defense in Depth: graduated protections in layers spanning application, platform and communication architecture

Defining Domains: a topological definition of protection by requirement where constituent elements are subject to consistent policy and protection mechanisms

Identity Management: comprehensive and definitive naming of system elements to allow application and assurance of security mechanisms

Simple Trusted Components: a preference for atomic protection mechanisms and system elements

Authorizing Operations: the ability to adjust the scope and depth of protection to meet stakeholder security concerns

Separation: segregating protection domains and mediating their exchange of information, control and authority

Auditing: facility for threat identification and classification supporting forensics and ongoing policy review and evolution

Linking Roles & Domains: cascading authentication and separation of domains to attenuate privileges

Complete Mediation: assured system-wide application and enforcement of protection mechanisms

Least Privilege: preferring that domain access spans the minimum range feasible to support required functionality

Few Trusted Components: minimal and symmetric formulation of criteria, privilege and protection across domains

Assurance: evidence based monitoring of policy and protection mechanisms across domains

Risk Management: dynamic policy and protection specification supporting timely response to the changing threat landscape and evolving stakeholder intentions

Manageable Access: coherent and user-accessible policy and protection mechanisms to manage and monitor domains

Security Principles and Protocols Grouped by the Choice Property They Express

“Trustworthy” Systems Theory

“objective” structural

“subjective” aesthetic

trustworthy

Defense in Depth

Elegance

Identity Management

intuitiveness

effectiveness

Authorizing Operations

usability

Auditing

vitality

robustness

divisibility

Defining Domains

Simple Trusted Components

factorability

scalability

constructibility

Separation

Linking Roles and Domains

Least Privilege

sustainability

predictability

Complete Mediation

Few Trusted Components

fidelity

Risk Management

confidence

Assurance

Manageable Access

Conclusion

- This is only a first step toward a design theory for trustworthy information systems.
- Pedagogical applications of Thriving Systems Theory have shown positive results in improving student design performance but, we have no “industrial-strength” experience to this point.
- Our next step is to develop a choice-property guided design methodology - ideally for artifact design and implementation in the “field.”
- Framing security design through a lens of Thriving Systems Theory informs the security intentions and security mechanisms encompassing stakeholder, policy maker, and developer.
- Our focus on artifact resonance with stakeholder intentions defines trustworthiness as a product of a subjective and objective portfolio of design concerns that must be managed in harmony.

discussion

LWaguespack@Bentley.edu

HICSS47 - Towards a Design Theory for Trustworthy Information Systems
Bentley University, Waltham, Massachusetts, USA
Leslie J. Waguespack, David J. Yates & William T. Schiano
lwaguespack@bentley.edu dyates@bentley.edu wschiano@bentley.edu

Trustworthiness: artifact resonance with stakeholder intentions as a product of a subjective and objective portfolio of design concerns managed in harmony.

Thriving Systems Theory Choice Property	Design Action	Action Definition	Security Design Aspect
Modularization	modularize	employing or involving a module or modules as the basis of design or construction	**Defining Domains**: a topological definition of protection by requirement where constituent elements are subject to consistent policy and protection mechanisms
Cohesion	factor	express as a product of factors	**Simple Trusted Components**: a preference for atomic protection mechanisms and system elements
Encapsulation	encapsulate	enclose the essential features of something succinctly by a protective coating or membrane	**Separation**: segregating protection domains and mediating their exchange of information, control and authority
Composition of Function	assemble	fit together the separate component parts of (a machine or other object)	**Linking Roles & Domains**: cascading authentication and separation of domains to attenuate privileges
Stepwise Refinement	elaborate	develop or present (a theory, policy, or system) in detail	**Defense in Depth**: graduated protections in layers spanning application, platform and communication architecture
Scale	focus	(of a person or their eyes) adapt to the prevailing level of light [abstraction] and become able to see clearly	**Least Privilege**: preferring that domain access spans the minimum range feasible to support required functionality
Identity	identify	establish or indicate who or what (someone or something) is	**Identity Management**: comprehensive and definitive naming of system elements to allow application and assurance of security mechanisms
Patterns	pattern	give a regular or intelligible form to	**Few Trusted Components**: minimal and symmetric formulation of criteria, privilege and protection across domains
Programmability	generalize	make or become more widely or generally applicable	**Authorizing Operations**: the ability to adjust the scope and depth of protection to meet stakeholder security concerns
User Friendliness	accommodate	fit in with the wishes or needs of	**Manageable Access**: coherent and user-accessible policy and protection mechanisms to manage and monitor domains
Reliability	normalize	make something more normal, which typically means conforming to some regularity or rule	**Complete Mediation**: assured system-wide application and enforcement of protection mechanisms
Correctness	align	put (things) into correct or appropriate relative positions	**Assurance**: evidence based monitoring of policy and protection mechanisms across domains
Transparency	expose	reveal the presence of (a quality or feeling)	**Auditing**: facility for threat identification and classification supporting forensics and ongoing policy review and evolution
Extensibility	extend	render something capable of expansion in scope, effect, or meaning	**Risk Management**: dynamic policy and protection specification supporting timely response to the changing threat landscape and evolving stakeholder intentions
Elegance	coordinate	bring the different elements of (a complex activity or organization) into a relationship that is efficient or harmonious	**Elegance**: protection mechanisms effectively, efficiently, and simply organized, realizing a security policy resonating with the stakeholder community's conception of security and welfare

Abbreviated Bibliography

Alexander C. The Nature of Order An Essay on the Art of Building and the Nature of the Universe: Book I - The Phenomenon of Life, The Center for Environmental Structure, Berkeley, CA, 2002.

Bell, D. E., & LaPadula, L. J. "Secure Computer Systems: Mathematical Foundations," Technical Report Mitre-2547, Vol. 1, Bedford, MA, USA, 1973.

Bishop, M. Computer Security: Art and Science, Addison-Wesley, Boston, MA, 2003.

Brooks F. P. "No Silver Bullet: Essence and Accidents of Software Engineering," Computer, 20(4), 1987, pp. 9-19.

Lampson, B. W. "Computer Security in the Real World," Computer, 37(6), 2004, pp. 37-46.

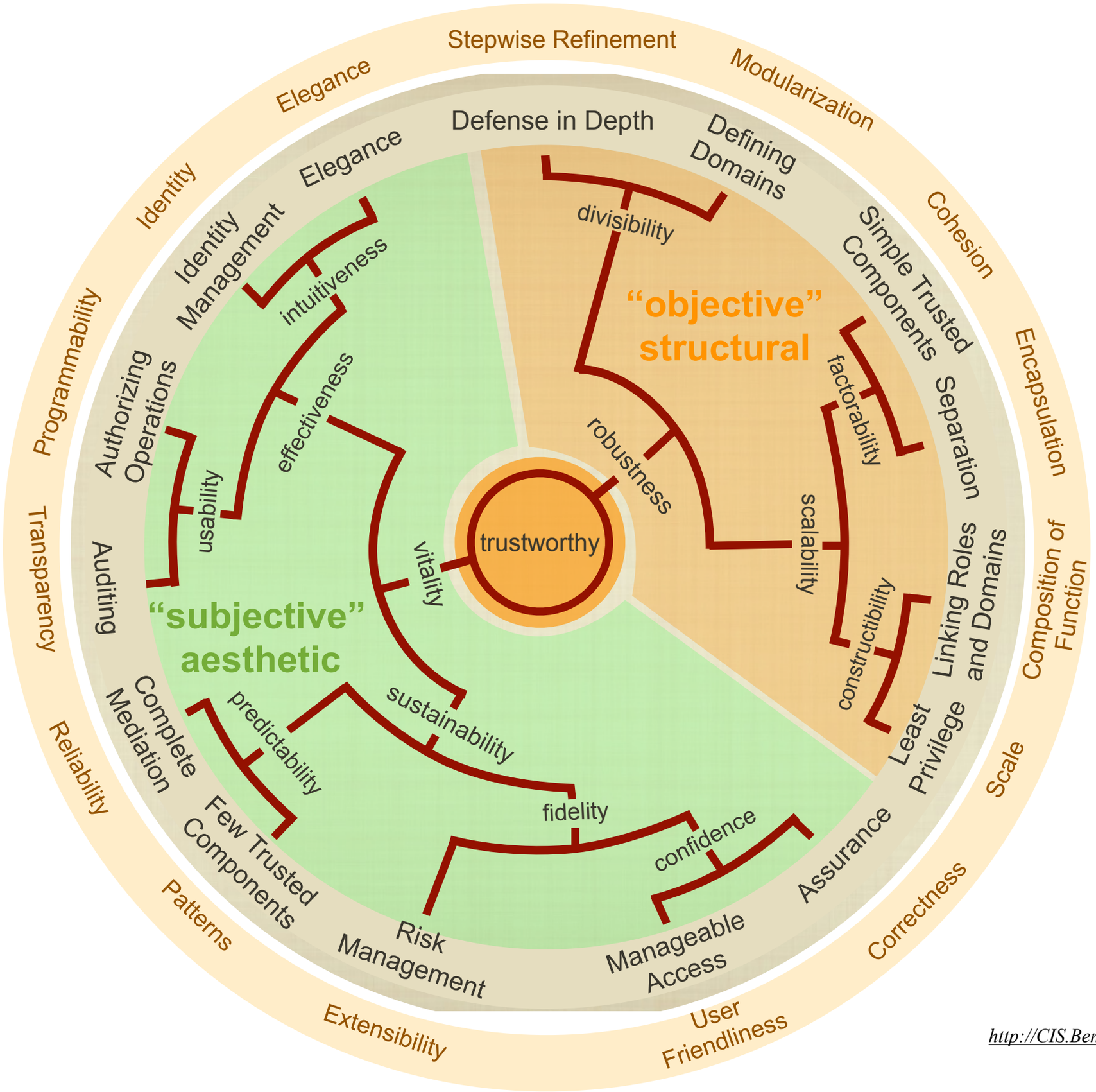
OECD. "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security," OECD, 2002, www.oecd.org/sti/ieconomy/1946962.doc, retrieved 20 August 2014.

Saltzer, J. H., & Schroeder, M. D. "The Protection of Information in Computer Systems," Proceedings of the IEEE, 63(9), 1975, pp. 1278-1308.

Waguespack, L. J. Thriving Systems Theory and Metaphor-Driven Modeling, Springer, London, UK, 2010.

Waguespack, L. J., & Schiano, W. T. "Thriving Systems Theory: An Emergent Information Systems Design Theory," in 46th Hawaii International Conference on Systems Sciences, 2014, pp. 3757-3766.

HICSS47 - Towards a Design Theory for Trustworthy Information Systems
Bentley University, Waltham, Massachusetts, USA
Leslie J. Waguespack, David J. Yates & William T. Schiano
lwaguespack@bentley.edu *dyates@bentley.edu* *wschiano@bentley.edu*



Thriving Systems Theory provides a vocabulary and framework for identifying and harmonizing security concerns in design decisions that align mechanisms with intentions to engender stakeholders' trust in information systems.

By categorizing security protocols of policy and mechanism aligned with TST choice properties, stakeholders and designers can dynamically tune the balance of functionality with structures that protect confidentiality, integrity and availability. That balance produces a qualitative resonance, the experience of trustworthiness that combines the subjective (aesthetic) with the objective (computational) stakeholder expectations.

http://CIS.Bentley.EDU/LWaguespack/docpdffiles/HICSS47SLIDES.pdf

A Special Ontology of Design

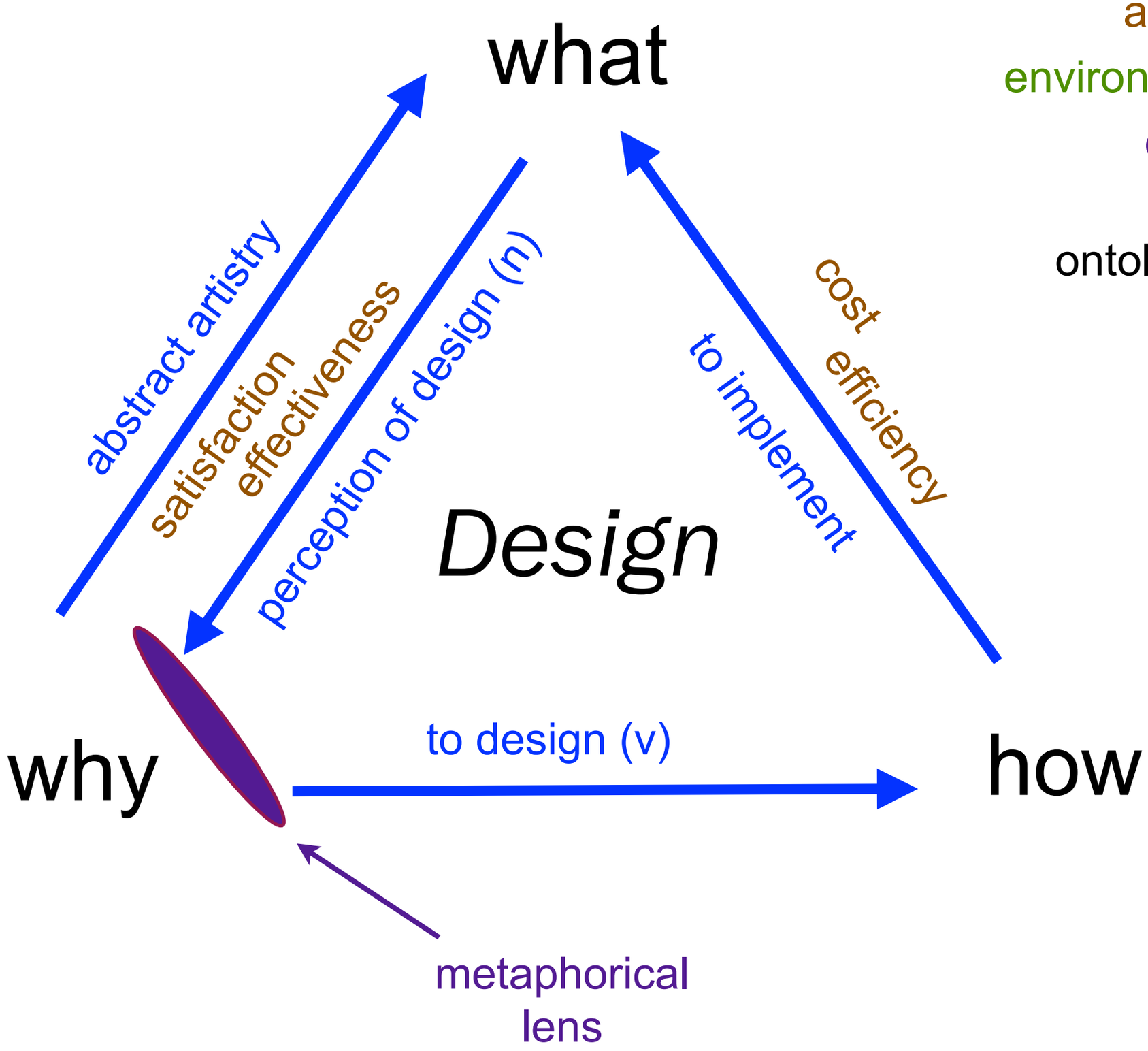
generative activity

activity affect

environmental parameter

conceptual metaphor

ontological primitive



A Special Ontology of Design

generative activity

activity affect

environmental parameter

conceptual metaphor

ontological primitive

system

edifice

model

artifact

what

abstract artistry

satisfaction

effectiveness

perception of design (n)

cost

efficiency

to implement

innovation

craft

scientific knowledge

culture

belief

why

purpose

need

intention

to design (v)

metaphorical lens

how

process

method

- A special ontology of design
  - constructs: why, how, what
    - The Why establishes the purpose of the artifact based on the intention and mindset of the designer
    - The How determines the mode of implementation of the artifact as process or methodology
    - The What is the product of the implementation that is the design effort's attempt at addressing the intention
  - relationships
    - the Why informs the How through design (v)
    - the How produces the What as artifact, edifice, model or system
    - the Why perceives the What's characteristics
    - the implementation of What bypassing design(v) might be called artistry where the intention is rendered directly in the artifact (given that any material art product involves some implementation if not "design(v)")
  - modifiers
    - the Why is conditioned by scientific knowledge, culture and/or belief in forming intention
    - the conceptual metaphor is the designer's mental model characterizing both the objective and subjective constructs to be produced in What by How
    - the conceptual metaphor translates the Why through design (v) to instruct the How
    - the How implements the What incurring cost and exhibiting efficiency
    - the What's design(n) characteristics are perceived by the Why through the conceptual metaphor to interpret the What's characteristics to exhibit satisfaction and/or effectiveness
    - the How is conditioned by existing craft that may be altered with implementation experience through innovation
- The metaphorical lens is both the source of instruction between the Why and How as well as the standard for interpretation from which the assessment of satisfaction will be realized
- It's interesting to note that although the characteristics of What seem to be the focus of design(v), only How is engaged directly with Why. It is as though How is the object of design rather than What. What simply provides the test case (the design(n)) that is evaluated as consistent or not against the Why, the result of the conveyance of Why's intention to How!?

Organizations design artifacts.

Organizations design processes.

Perhaps the most important artifact organizations should design is “why they design!”