Trust = Utility + Security: Designing for that Elusive Quality in Cloud Computing

Les Waguespack, Ph.D., Professor
William T. Schiano, DBA, Professor
David J. Yates, Ph.D., Associate Professor

Computer Information Systems
Bentley University
Waltham Massachusetts

Design Principles & Practices - Chicago
March 12, 2015
**Premise**

- **Trust** in any information system is a snapshot in a dynamic amalgam of diverse objective and subjective factors:
  1. an evolving and diverse population of stakeholders
  2. advancing technological opportunities for protection
  3. a changeable environment of personal social and economic values
  4. the increasing ingenuity and guile of adversaries
  5. the theoretical and practical capacity for assurance

- “Many of the features that make cloud computing attractive […] can also be at odds with traditional security models and controls.”
  
  *(Jansen and Grance 2011)*

- Design must attend to objective and subjective perceptions of form and function:
  1. to enable stakeholders to integrate their broad range of security concerns and the potential responses
  2. in a balance that satisfies stakeholders’ conception of both utility and security.
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

Security in Information Systems
Statement of requirements that explicitly defines the security expectations of the mechanism(s)

Security in Information Systems
Assurance Engenders Trust

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

Policy

Assurance

Mechanisms

The objective, computational elements implementing the “physical” security model
The subjective, intention of the stakeholders defining satisfactory behavior

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

The objective, computational elements implementing the “physical” security model

Security Management Sustains Trust
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.
Design Choice Properties in Confluence Experienced as Design Quality
Thriving Systems Theory

“subjective” aesthetic

“objective” structural

- Elegance
- Identity
- Intuitiveness
- Effectiveness
- Usability
- Vitality
- Sustainability
- Fidelity
- Confidence
- User friendliness
- Reliability
- Transparency
- Predictability
- Patterns
- Extensibility
- Correctness
- Stepwise Refinement
- Modularization
- Divisibility
- Robustness
- Scalability
- Constructibility
- Factorability
- Composability
- Functionality
- Correctness
- Transparency
- Programmability
- Extensibility

- Thriving

©LJW, 2015 All Rights Reserved
Security Principles and Protocols Grouped by the Choice Property They Express
Security Design Aspects

**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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Grouped by the Choice Property They Express**
“Trustworthy” 
Systems Theory

“objective” 
structural

“subjective” 
aesthetic

Defense in Depth
Defining Domains

Simple Trusted Components
Separation

Least Privilege
Assurance

Manageable Access
Risk Management

Few Trusted Components
Complete Mediation

Auditing
Authorizing Operations

trustworthy

trustworthy Systems Theory

Elegance
Intuitiveness
Effectiveness
Usability
Sustainability
Vitality
Fidelity
Confidence
Robustness
Scalability
Constructability
Factorability
Divisibility

©LJW, 2015 All Rights Reserved
There is no unique algorithm or optimal set of design guidelines for security.

A sound design theory for information systems will alleviate many problems (i.e. poor communication among cloud service providers, clients and stakeholders).

Trust among cloud tenants proceeds from clarity of expectations integrated and balanced in design.

Thriving Systems Theory provides a design framework that focuses on artifact design choices that resonate with stakeholder intentions – both objective and subjective.

Our contribution to the quality of trust in cloud computing is a design theory focused on artifact resonance with stakeholder intentions grounded on the imperative that systems architecture and security choices must not only accommodate but facilitate ongoing adaptation and change.
Published Design Domain Applications of Thriving Systems Theory

- Thriving Systems Theory and Metaphor-Driven Modeling
  - Springer-Verlag {2010}
- Choice Properties in Extant Systems
  - APACHE web server (JDM&P) {2013}
- Choice Properties Mapped to Modeling
  - agile methodology SCRUM (HICSS-45) {2012}
  - relational modeling (ontology) (ISEDJ) {2013}
  - systems design theory (HICSS-46) {2013}
  - security principles & protocols (HICSS-47) {2014}
  - object-oriented modeling (ontology) (ISEDJ) {2015}
discussion

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

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

Abbreviated Bibliography


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.