Measuring System Security

Doctoral Dissertation Defense

December 1, 2011

Jennifer L. Bayuk

Doctoral Candidate, School of Systems and Enterprises

Stevens Institute of Technology

Committee members:

Ali Mostashari, School of Systems and Enterprises (chair)

Brian Sauser, School of Systems and Enterprises

Paul Rohmeyer, Howe School of Technology Management

Barry Horowitz, University of Virginia

Background/Purpose of Research

- Today's security metrics support management practices rather than measure system capability to withstand attacks.
- This may work well for managing day-to-day security support operations, but does not work well in security tradespace calculations. In planning for system capabilities such as adaptation to threat, proactive deterrence, and resilience to attack, security features must be measured using engineering methods for verification and validation of system function.
- Security metrics should be useful in estimates of a security function's benefit in comparison with other system features.
- This research uses engineering tools and techniques to create a new category of security metrics: *system security metrics.*

Research Statement

The research question for the dissertation is:

How can system security be measured?

A Stake in the Ground

Measurement must have an object.

This observation led to the hypothesis for the dissertation, which is:

System security can be measured if and only if the system-level attributes of:

- *articulated mission and purpose,*
- *validated input, and*
- *incident detection and response*

contribute to that measurement.

Explicit Assumptions

- *System security is defined as a system attribute that that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.*
- *This definition is expressed in propositional logic as follows:*

  (For all A, (E(X,V(A)) ➔

  (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) AND T(B,P(Y,A)))

Constructing a Null Hypothesis

E(X,S) ←→ Exists (M,I,R) ((E(X,M) AND E(X,I) AND E(X,R)) ← system attributes from hypothesis

AND

(For all Y ((S(Y) AND (For all T, (C(Y,T) → (C(X,T)) ← define system-level attributes

AND

(Exists U (C(X,U) AND ~C(Y,U)))) →

(~(M = U) AND ~(I = U) AND ~(R = U)))

AND

(For all A, (E(X,V(A)) ➔ (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) ← definition of security

AND T(B,P(Y,A)))

The Null Hypothesis

Based on the observation that the hypothesis contains only system-level attributes, the null hypothesis assumes:

System security can be measured by measuring attributes of components.

School of Systems & Enterprises

Research Approach

Conceptualization

- Frame the measurement problem in terms of a theory of system attributes that contribute to security.

Data Collection

- Survey security experts to get their judgment on the attributes that contribute to a system-wide attribution of security, as well as the best way to measure system security.

Theory Development

- Utilize the judgment of experts in proposing a theoretical solution that can be tested with real-world experiments.

Case Study

- Apply the theoretical solution to case studies.

Hypotheses Validation

Survey Overview

Asked security experts questions to get their judgment on the "best" way to identify and measure system security attributes.

- Included questions that support hypothesis as well as questions in the survey to be considered "noise" for the purposes of ensuring that survey participants are not limited in their responses by expected conclusions.
- Institutional Review Board concerns:
  - Characteristics of subjects: System Security SMEs, no other criteria.
  - Plans for recruitment of subjects: Based on established industry credentials such as attendance at invite-only security expert workshops.
- Sample characteristics:
  - 224 potential respondents, 109 responded, or ~49%.
  - Not all respondents completed survey, inclusion criteria was based on coverage of ranked metrics, which yielded 60 usable surveys or ~27%.
  - Average years in security: 18, in technology: 26. Advanced degrees: ~66%.
  - Verified results with experts who expressed willingness to do so, of 19 such respondents, 6 provided feedback, or ~32%.

School of Systems&Enterprises

Survey Analysis

- Quantified the influence of demographically dominant financial industry group via Mann-Whitney tests for change in median, Kolmogorov-Smirnov test for a more general change of shape. Tests revealed significant differences for only one metric, which was left in after examination of the details.
- Identified questions for which collective responses approximated a flat or normal curve, which were taken as indications of ambiguity (a skew value below 0.3 and also a central median, or a kurtosis near zero). Eliminated seven potential security metrics.
- Rank ordered remaining results using three different techniques:
  - Thurstone
  - One Number
  - Survey Rank
- Clustered responses into four levels of importance.

Survey Results

- Security experts confirmed the importance of the hypothesized system-level metrics:
  - Metrics of high importance included: Articulate, maintain, and monitor system mission, System interfaces accept only valid input, Capability for incident detection and response.
- They further confirmed the importance of system-level metrics in general over component metrics:
  - Other metrics of high importance: Ability to withstand targeted penetration attacks by skilled attack teams, Personnel awareness, screening and supervision, Ability to evaluate the extent to which systems are protected from known threats.
  - Metrics of low importance: Percentage of systems or components that have passed security configuration tests, ability to maintain values of standard security variables in system technical configuration, ability to pass security audit.

Applied Survey Results *in red*

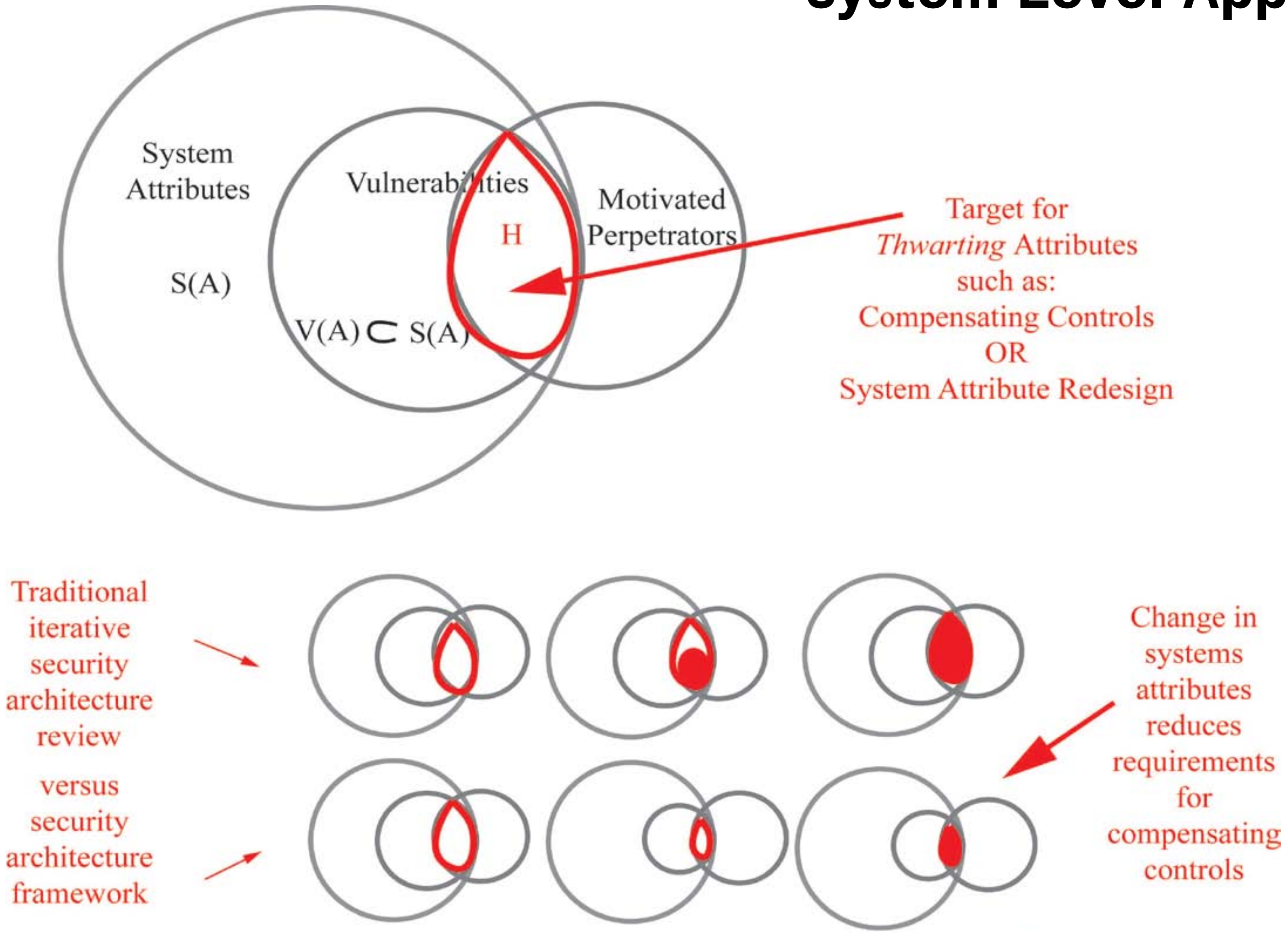
1. Secure systems contain an hypothesis attribute
2. Most important security attributes are at component level
3. Component attribute is not an hypothesis attribute
4. System exhibits security attribute
5. Hypothesis: System is Secure ←→ { 1 } AND { 2→3 } AND { 4 }

Truth table demonstrating experimental results effect on the hypothesis				
1	2	3	4	5
T	T	T	T	T
T	T	F	T	F
T	F	T	T	T
T	F	F	T	T
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	T	F

Hypothesis Validation

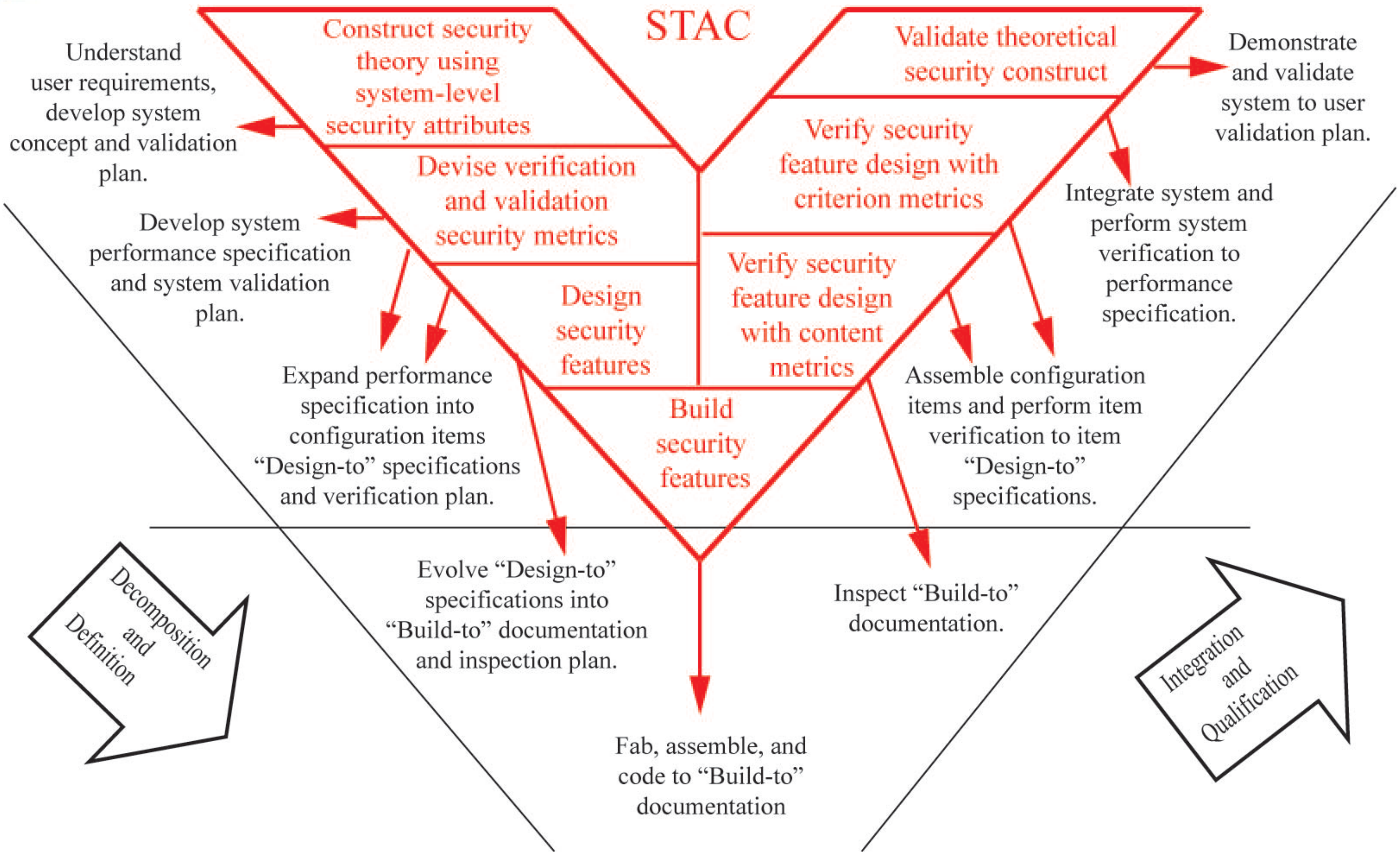
- The research hypothesis is an example of *construct theory*, requiring identification of relationships between security and measurable things that correlate with it. As no agreed-upon security metrics yet exist, this led to the nonparametric statistical approach of attitude measurement. The measured attitudes supported the hypothesis.
- Existing systems engineering practice of measuring a system by the aggregation of its components made the null hypothesis a valid statement using the standard of *content* validity.
- Restricting the survey sample to experts enhanced its validity using the standard of *criterion* validity, as experts may be expected to provide the criteria required for something to be called secure. Criterion candidates were presented in the form of both attributes of secure systems and methods of security measurement.
- The survey sample was analyzed to support conclusions of *internal* validity, but could be expanded to other communities in security-related professions to enhance expected *external* validity.

Graphical Illustration of the System Level Approach



Area of vulnerability is either reduced, or covered with security-specific bolt-ons.

Security Theory Attribute Construction Framework



Note: Vee model is based on Buede, 2009.

A Systems Thinking Approach

Checkland-STAC Overlay

1. Problem Situation Unstructured
2. Structured Problem Expression
3. System Definition
4. Conceptual Model

   Construct security theory using system-level security attributes

5. Comparison of the Model to the Structured Problem

   Devise verification and validation security metrics

6. Identify feasible changes in structure, procedure, and attitude

   Design security features

7. Recommend action to improve the situation

   Build security features

   Verify security feature design with content metrics

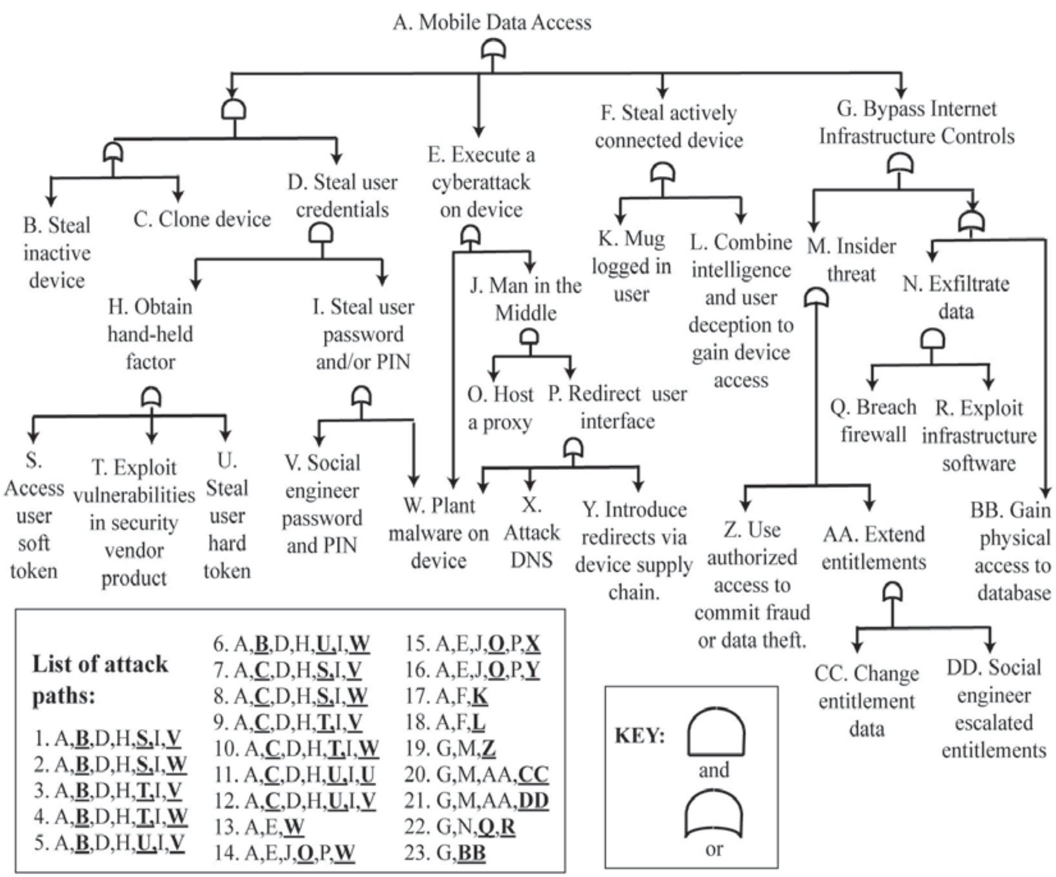
   Verify security feature design with criterion metrics

   Validate theoretical security construct

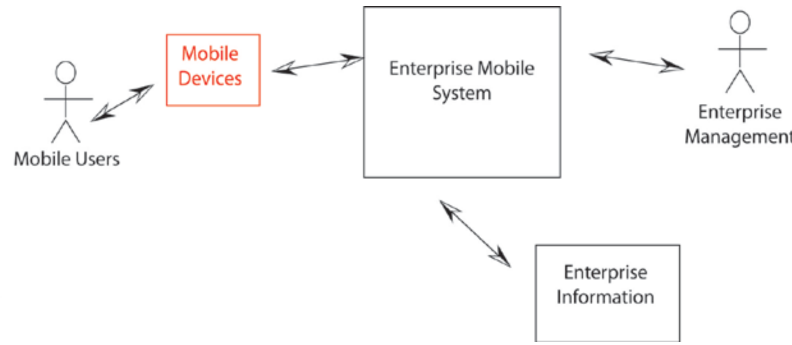
traditional security

Example Case Study: Mobile Communications

Structured Problem Expression

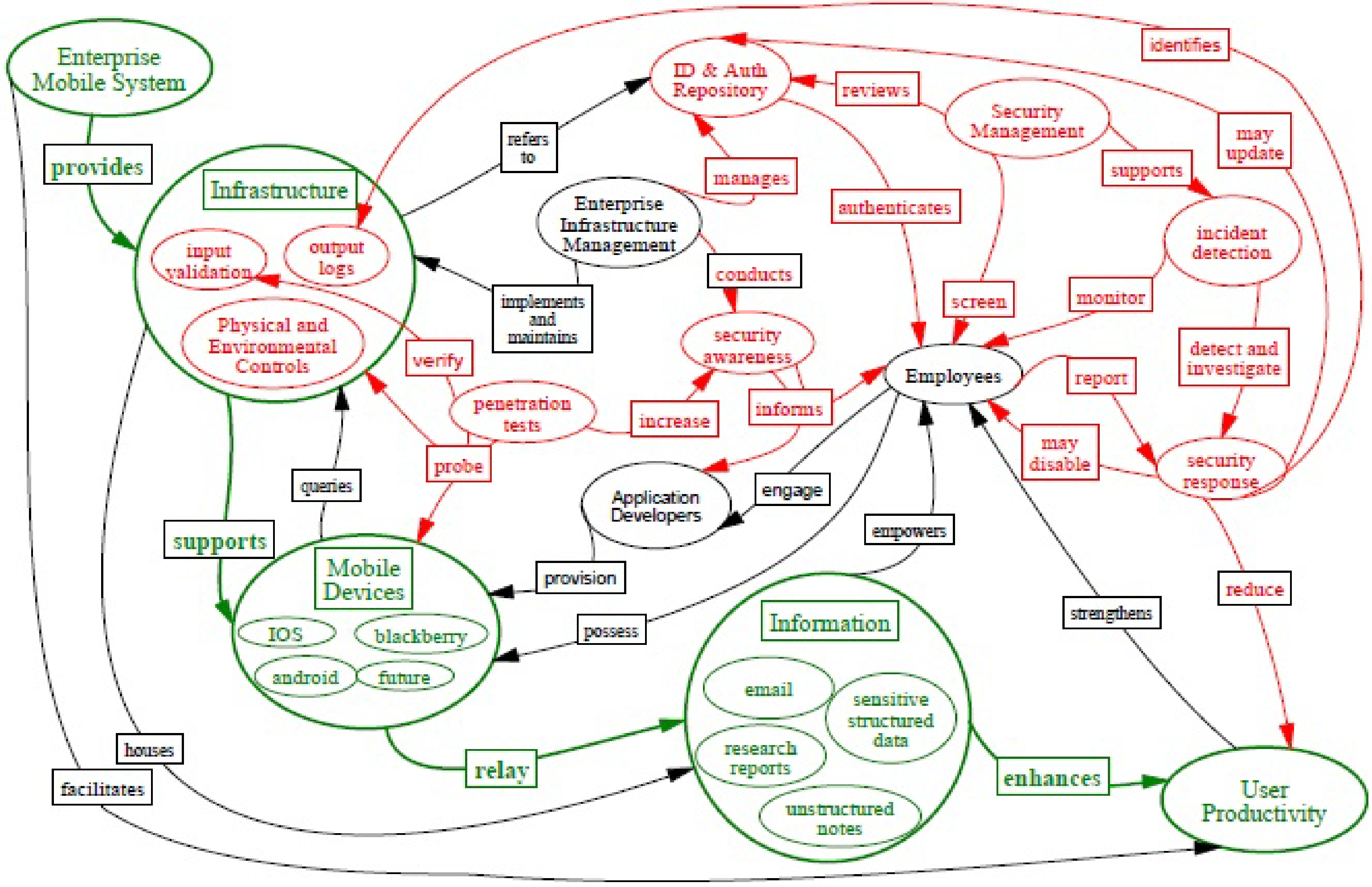


System Definition



Mobile Communications: Conceptual Model

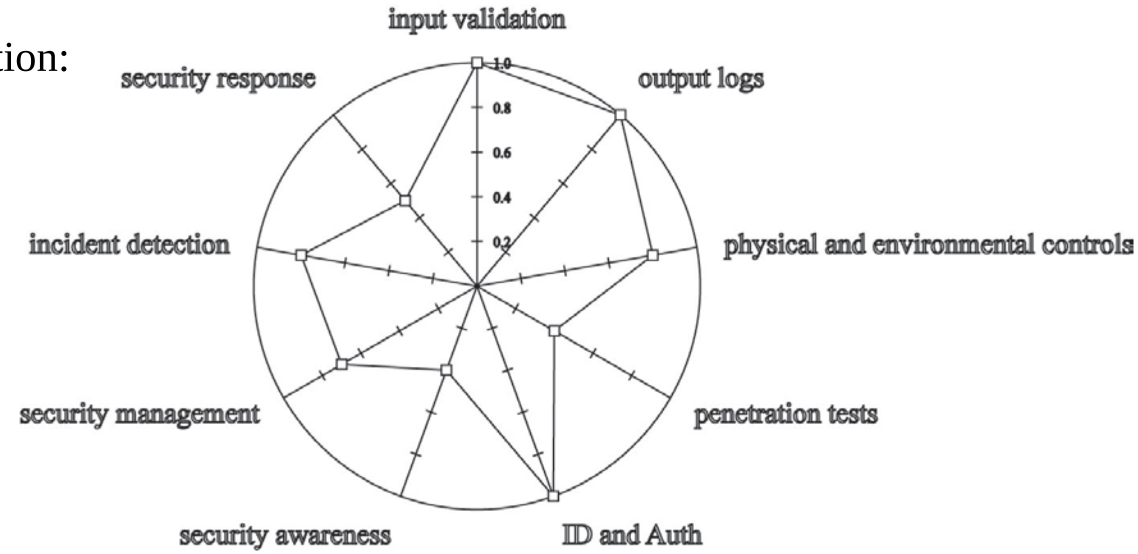
Construct security theory using system-level security attributes



Comparison of the Model to the Structured Problem

Devise verification and validation security metrics

Verification:



Validation:

Test	Result
MSWFR	23 minutes
Investigation data availability	Fail
Investigation data integrity	Pass
Unauthorized data download	Pass
Unauthorized access deterrents	Pass

STAC Validation

- Case studies provide anecdotal but not scientific validation for STAC.
- The systems engineering process of defining any system function in terms of components provides the way to test STAC security features using both *content* and *criterion* validity. These methods exploit existing security content and criterion metrics such as targeting 100% standards compliance and vulnerability testing. These are a necessary, though not sufficient, part of the overall *construct* theory testing process.
- Further application of the STAC theory is required to accumulate more test results and ensure that they correspond to the expert criterion. These results may also refine the criterion.
- Research result has face validity in that "system security should be measured at system-level" appears tautological, yet given today's emphasis on measuring security using generics standards, it may be expected to be resisted. This attitude will only be overcome by repeated and documented successful application of the result.

Research Contributions

- Literature – This dissertation's literature review in security metrics is the first to use scientific validity as a criteria for creating taxonomy.
- Conceptual – This research provides the field of security metrics with a sorely-needed paradigm shift toward systems thinking.
- Methodological - The STAC framework for success-oriented security validation encompasses and leverages existing security engineering tools and techniques, and provides a method to compare security among similar systems.
- Empirical – The research tested a theory about security metrics using a formal hypothesis and survey data, whereas prior research based conclusions about security on metrics without prerequisite foundational theoretical constructs.

School of Systems & Enterprises

Research Shortcomings

This work would have benefited from:

- More time and patience on the part of security subject matter experts.
- More granular definitions of security metrics questions to allow easier interpretation by subject matter experts.
- Multiple case studies in systems of similar mission and purpose to enable comparison of results using STAC-suggested guidance.

Future Work

This research will continue in a variety of forms, including but not limited to:

- Enlisting practicing systems engineers to incorporate the STAC method of security requirements and metrics into their mainstream requirements process and compare resulting sets of security verification and validation metrics.
- Production of detailed systems engineering guidance for turning system-level security requirements into concepts of operations.
- Comparison of systems security education curriculum at the component versus system level, and corresponding evaluation as appropriate for educational objectives.

School of Systems & Enterprises

Summary

- System-level security matters.
- Security subject matter experts concur.
- Systems engineers should decide what they need to measure to determine that security exists for the given system of interest before deciding what features are needed to implement security.
- The *Security Theory Attribute Construction Framework* provides guidance for those who would attempt this approach.

School of Systems&Enterprises

Publications

Title	Venue	Date
The Utility of Security Standards	International Carnahan Conference on Security Technology	October, 2010
Systems Security Engineering	IEEE Security and Privacy	Apr-Mar, 2011
Security Verification and Validation *with Brian Sauser and Ali Mostashari*	Conference on Systems Engineering Research	April 2011
Systems of Systems Issues in Security Engineering	INCOSE Insight	July 2011
An Architectural Systems Engineering Methodology for Addressing Cyber Security *with Barry Horowitz*	Systems Engineering	Volume 3, 2011
Cloud Security Metrics	IEEE SoSE Conference	June 2011
Measuring Cyber Security in Intelligent Urban Infrastructure Systems *with Ali Mostashari*	Conference on Emerging Technologies for a Smarter World	November 2011
Security Metrics for Systems Engineers *with Ali Mostashari*	Accepted by Systems Engineering	TBD 2012
Security Decision Theory *with Paul Rohmeyer and Tal Ben Zvi*	In draft format, venue TBD	