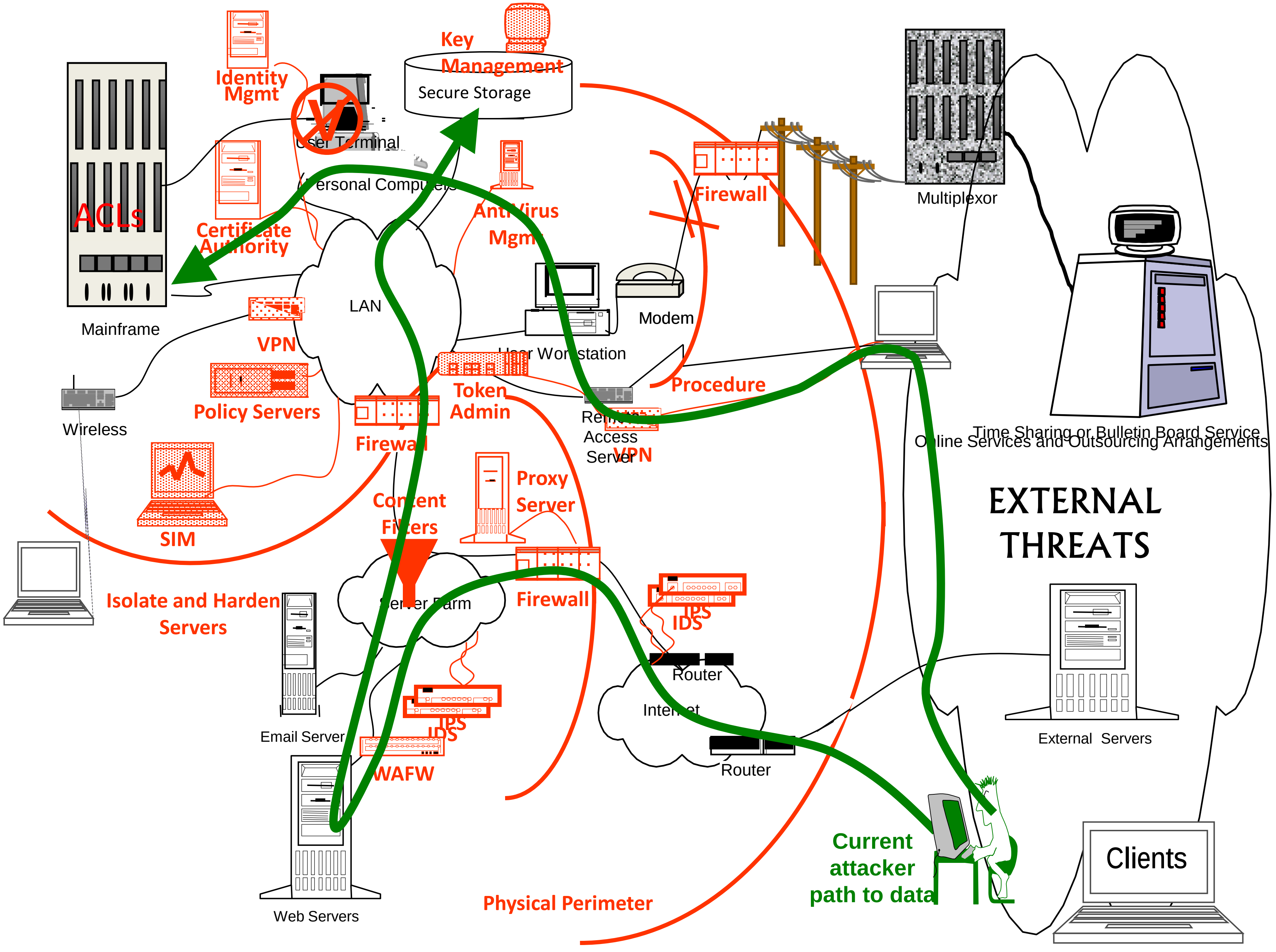
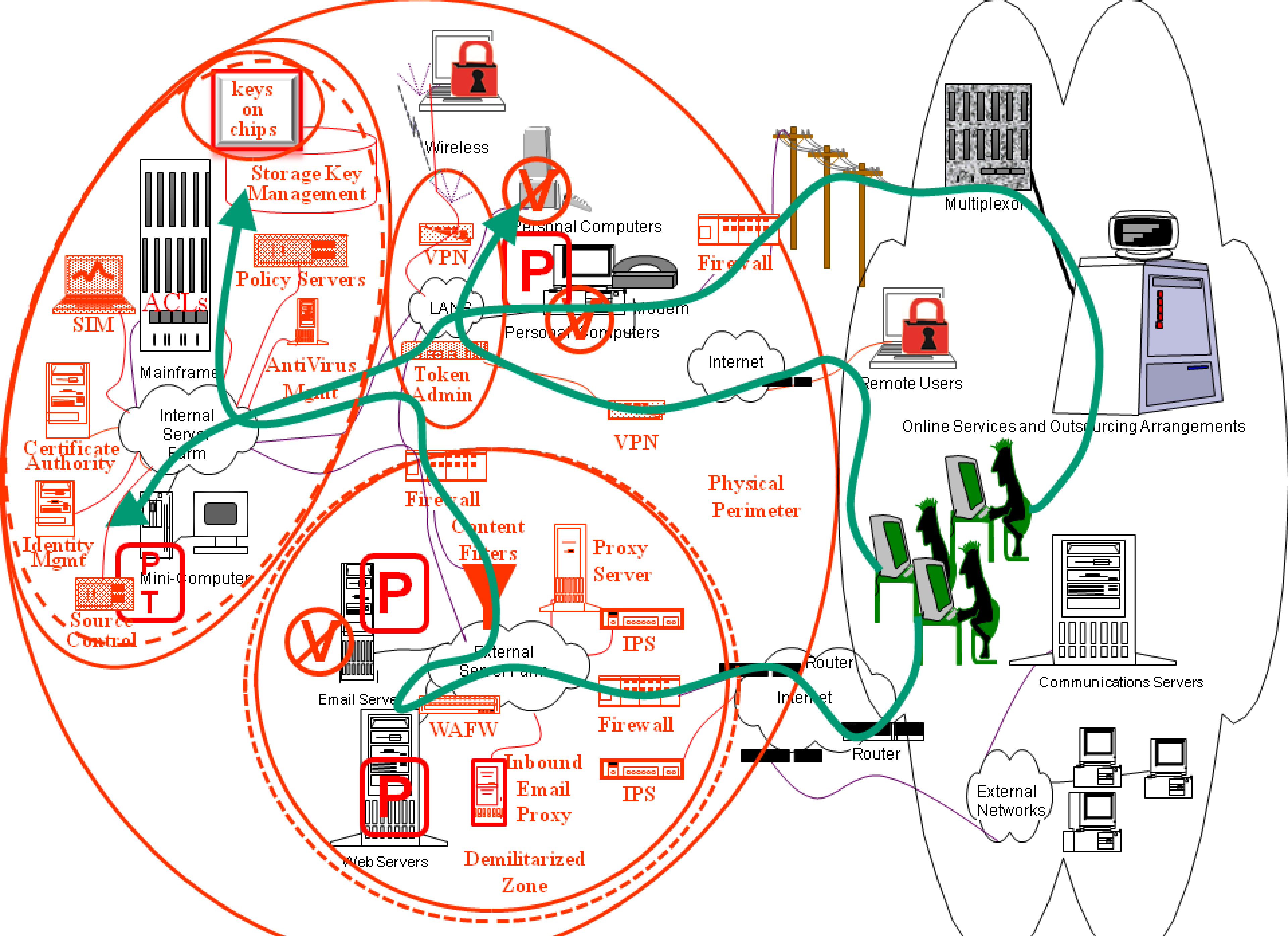
Measuring System Security

For NY SPIN

By:

Jennifer Bayuk


Key
Management
Secure Storage
Identity
Mgmt
User Terminal
Personal Computers
ACLs
Certificate
Authority
Anti Virus
Mgmt
Mainframe
LAN
VPN
Policy Servers
Token
Admin
Firewall
User Workstation
Modem
Firewall
Multiplexor
Procedure
Remote
Access
Server
VPN
Time Sharing or Bulletin Board Service
Online Services and Outsourcing Arrangements
Wireless
SIM
Content
Filters
Proxy
Server
Isolate and Harden
Servers
Server Farm
Firewall
IPS
IDS
Router
Internet
Router
Email Server
IPS
IDS
WAFW
Web Servers
EXTERNAL
THREATS
External Servers
Current
attacker
path to data
Physical Perimeter
Clients



Source: J. Bayuk, J. Healy, P. Rohmeyer, M. Sachs, J. Schmidt and J. Weiss, Cyber security policy guidebook, Wiley, forthcoming, 2012.

System Security Metrics

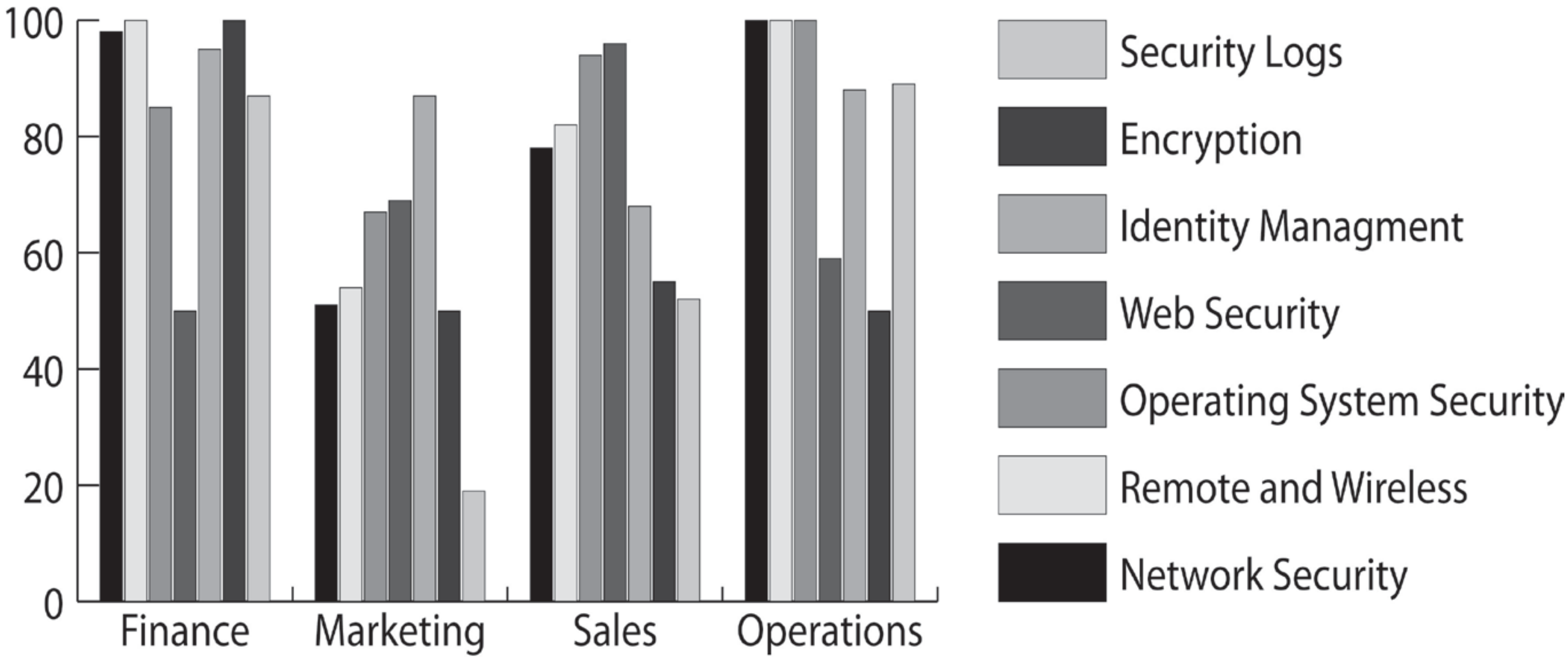
System security may comply with security standards, yet still not serve the mission of a given enterprise

- Security professionals call this: correct versus effectiveness (C&E)
- Certification authorities call this: security testing and evaluation (T&E)
- Engineers instead use: verification and validation (V&V)

C, T, V_1 *Did we build the system right?*
Are the specifications met?

C, T, V_2 *Did we build the right system?*
Does the design work?

Target Security Metrics



Ratio

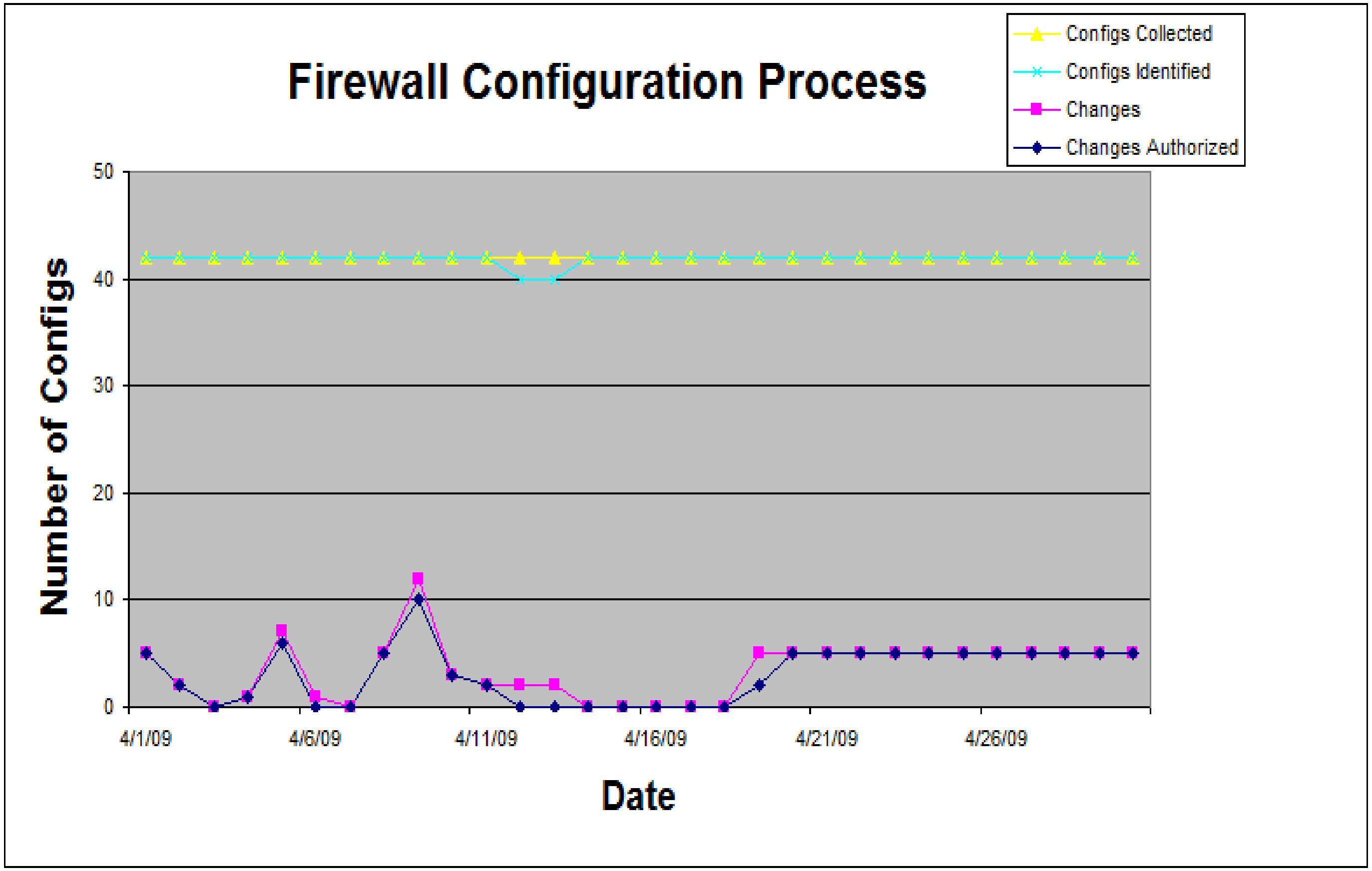
Automated

Accurate	Numeric	Correct	Consistent	Time-based	Replicable	Unit-based	Informative	Overall
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Strong

Good verification indicator

Monitoring Metrics

Interval



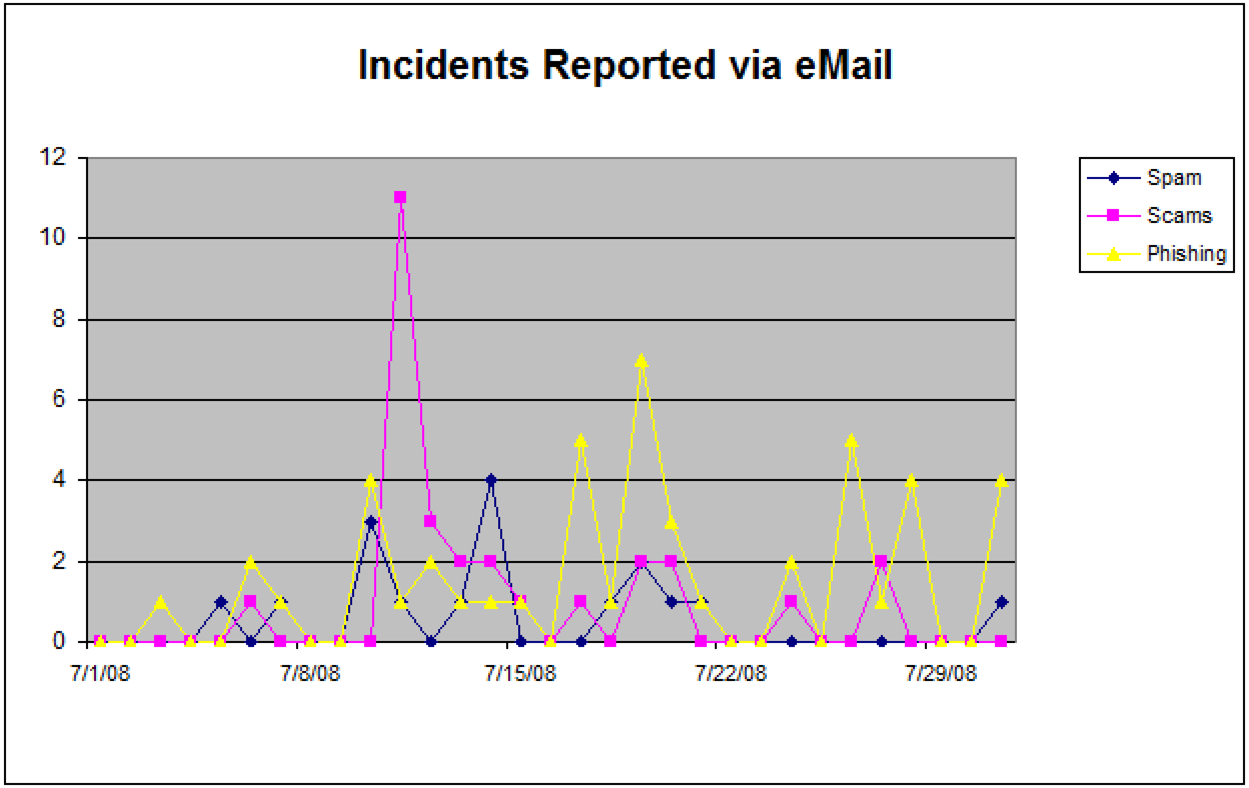
Manual

Accurate	Numeric	Correct	Consistent	Time-based	Replicable	Unit-based	Informative	Overall
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Strong

Process-level verification indicator

Activity Metrics

Interval



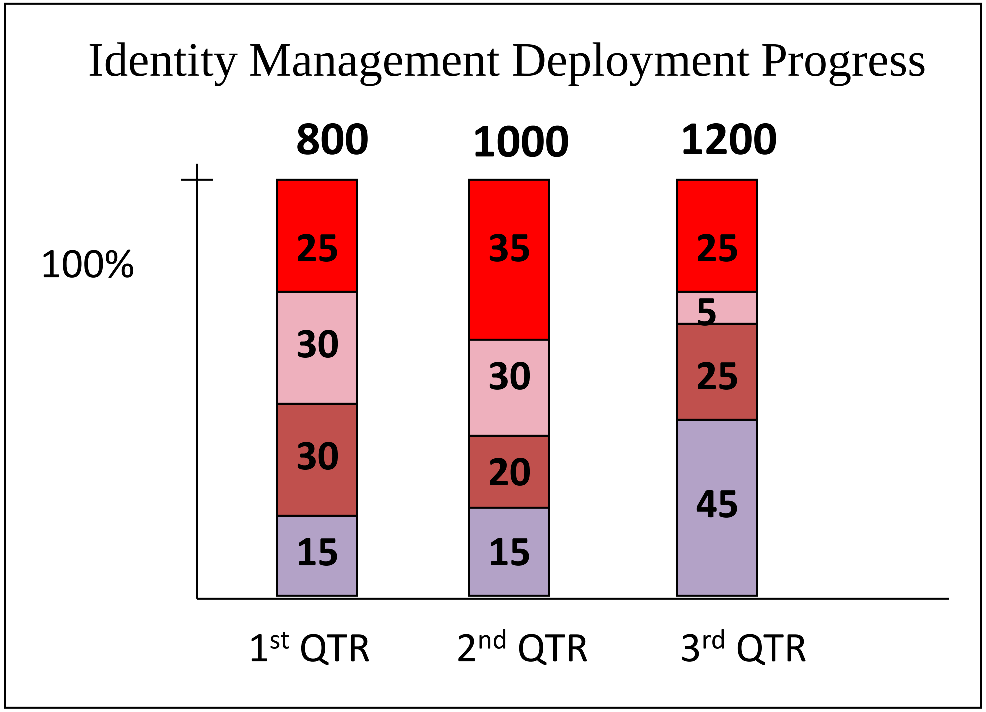
Manual

Note: blank lines indicate no incidents were reported, mostly weekends.

Accurate	Numeric	Correct	Consistent	Time-based	Replicable	Unit-based	Informative	Overall
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Weak

Measures only external environment, not system response

Remediation Metrics



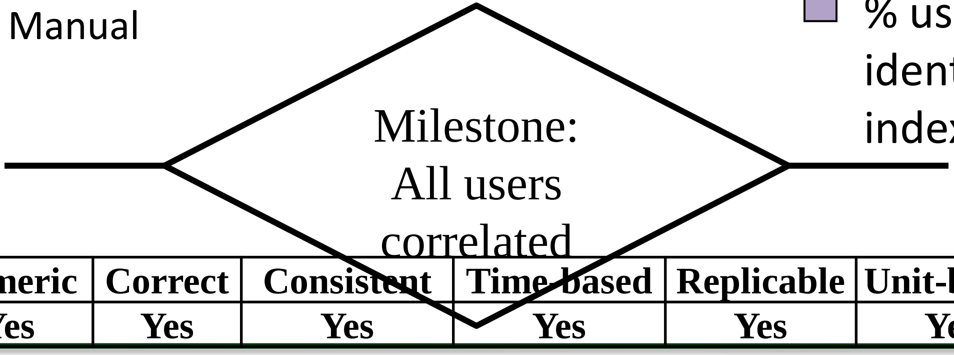
🟥 estimated % not yet identified

▨ % users that are not mapped to an existing and valid identity

🟫 % users known to map to an existing and valid identity, but are not configured to automatically correlate to an identity management system index

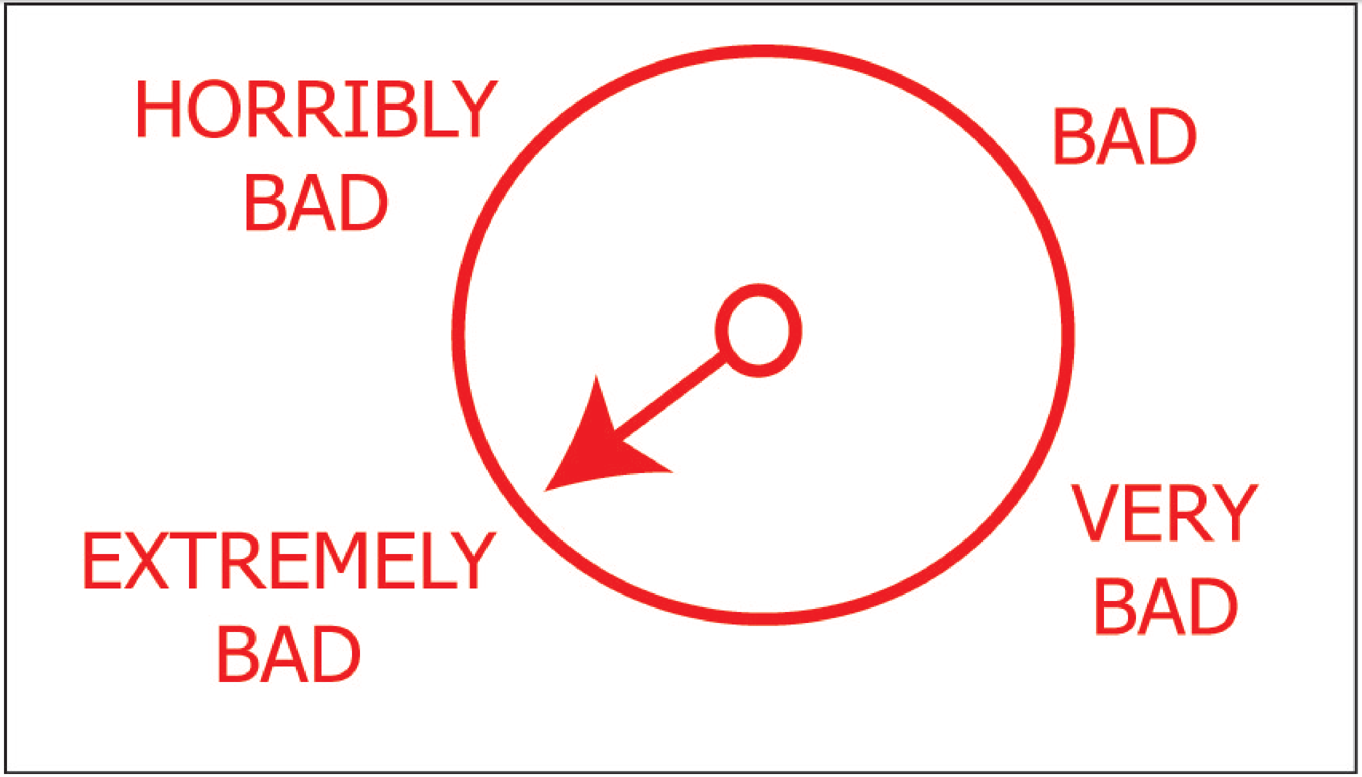
🟪 % users that correlate to an identity management system index

Interval Manual



Accurate	Numeric	Correct	Consistent	Time-based	Replicable	Unit-based	Informative	Overall
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	?

Vulnerability Metrics

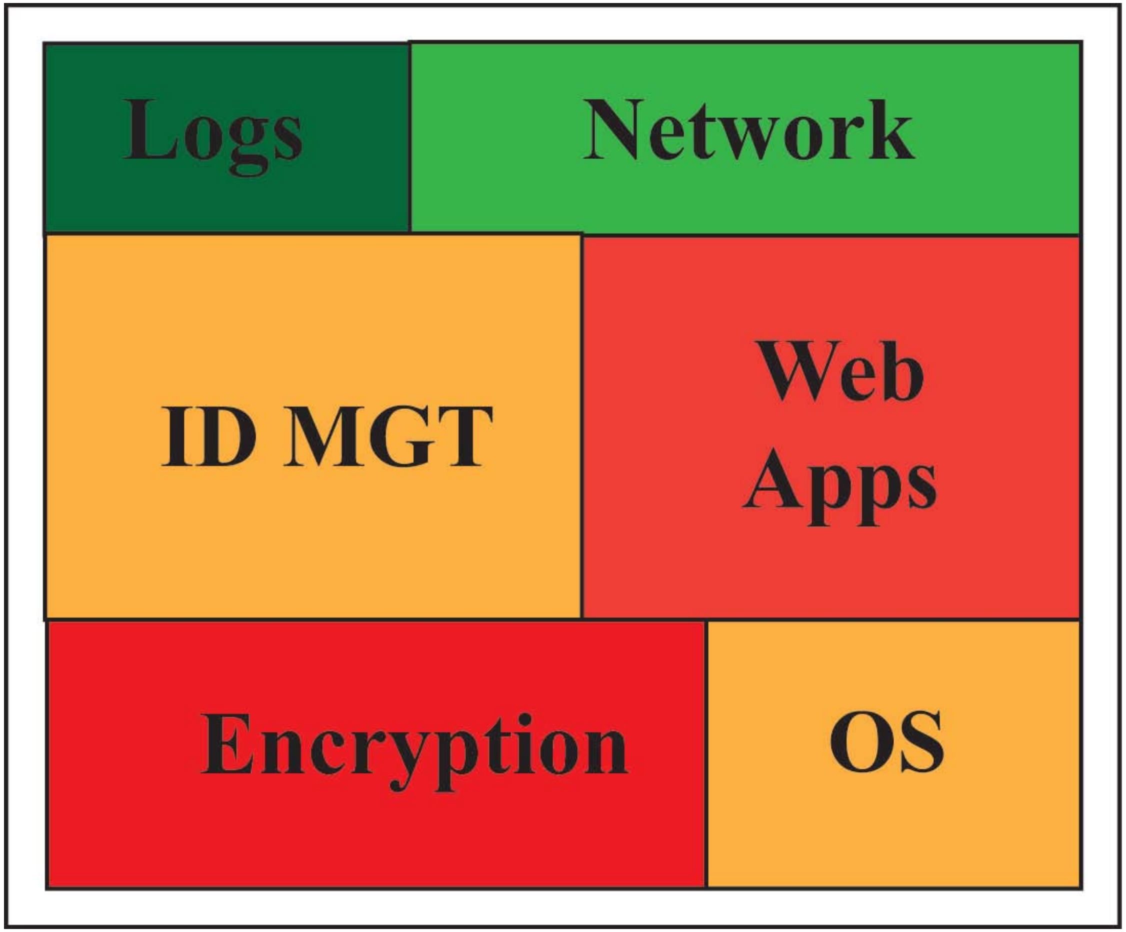


“Badness-ometers” – Gary McGraw

Accurate	Numeric	Correct	Consistent	Time-based	Replicable	Unit-based	Informative	Overall
?	No	?	No	Yes	No	No	Yes	Weak

Not reliable or repeatable

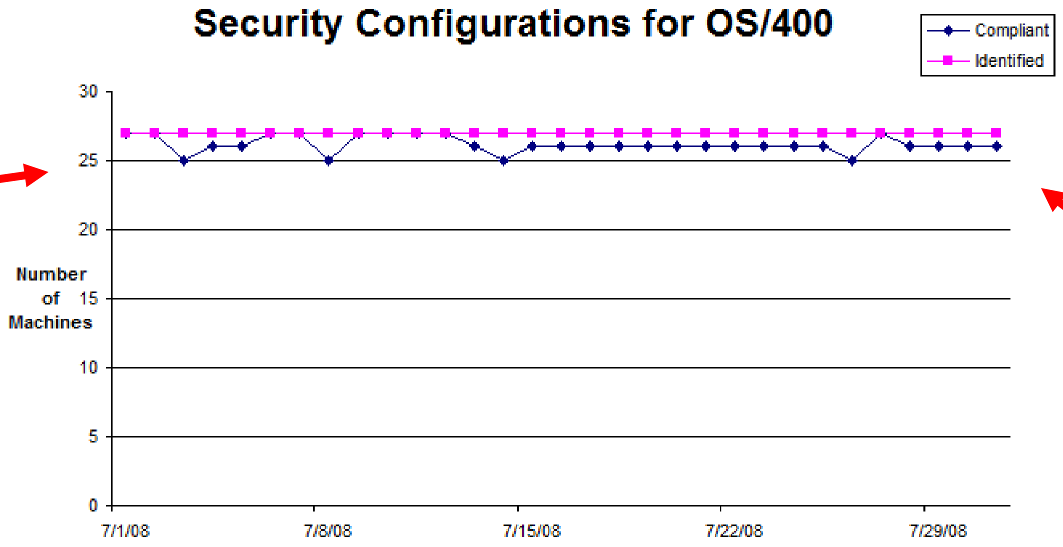
Typical Security Metrics "Risk" Dashboard



Risk versus Security Metrics

Assessment vs Implementation

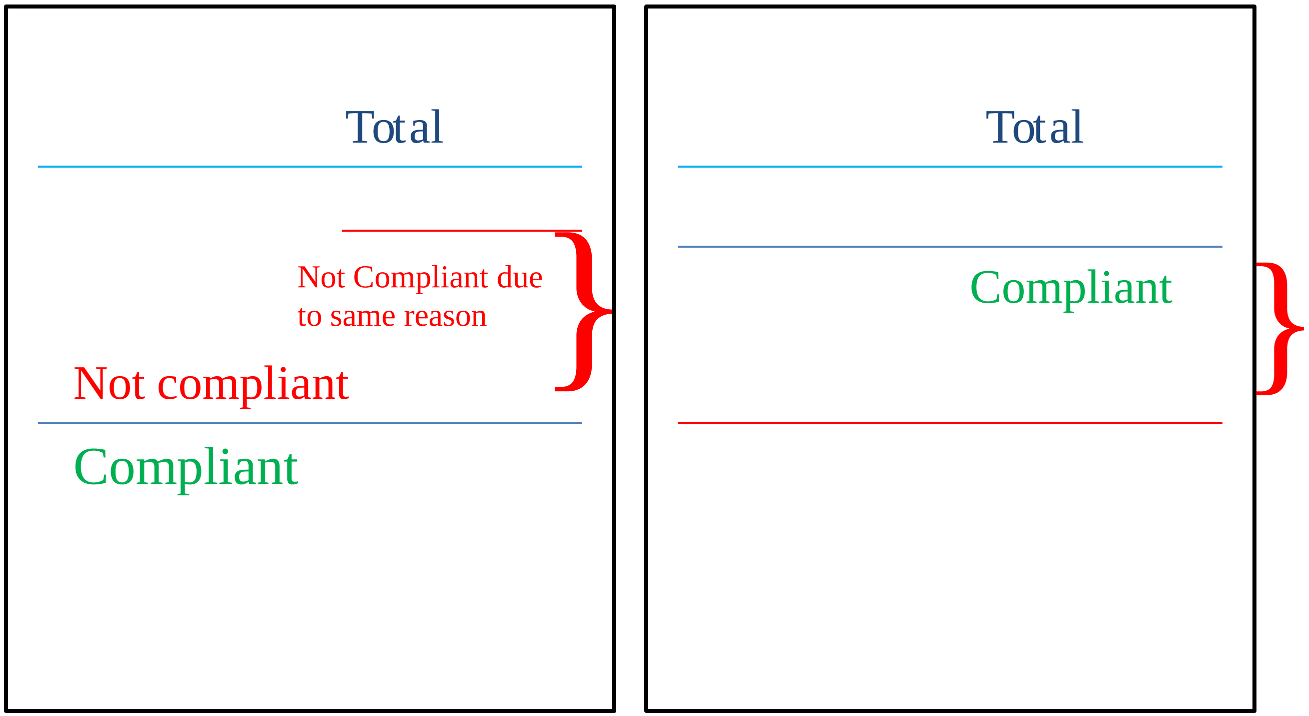
Risk manager see no dramatic changes



Security manager sees systemic issue

Potential Conflict of Interest

Solution: Declare reason not a risk



Total

Not Compliant due to same reason

Not compliant

Compliant

Total

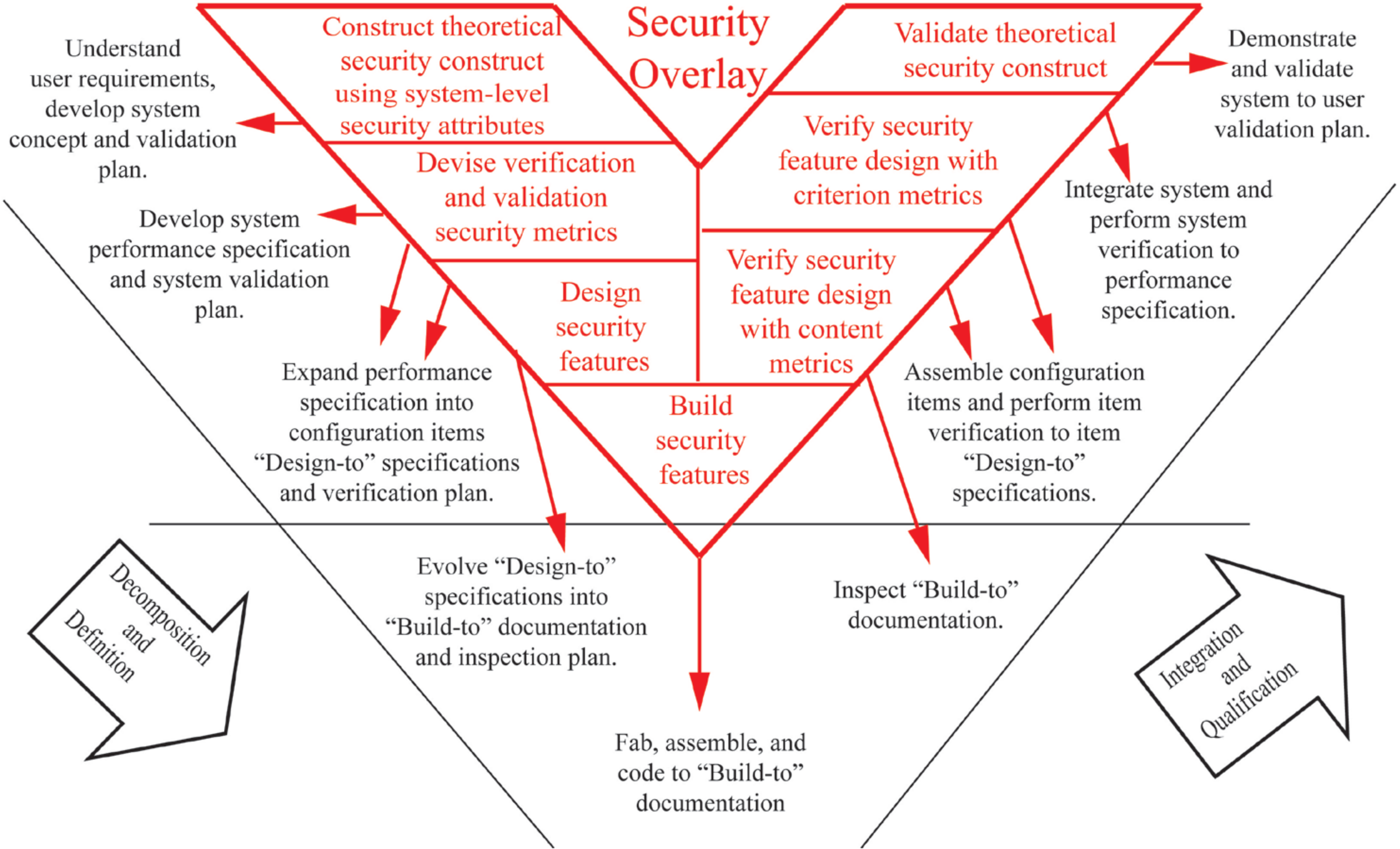
Compliant

Risk Managers may be tempted to accept unsecure configurations which would make seemingly technical charts look different to management.

Current Security Metrics

- Apply standard criteria to an enterprise security program to determine its security strength
- Measure process rather than results
- Concentrate on security risk, the cost of controls, and the expected benefit of return on discreet security investments
- Pass Correctness, Test, and Verification, but fail on Effectivenss, Evaluation, and Validation

An Engineering Approach



Security Overlay

Construct theoretical security construct using system-level security attributes

Devise verification and validation security metrics

Design security features

Build security features

Verify security feature design with content metrics

Verify security feature design with criterion metrics

Validate theoretical security construct

Understand user requirements, develop system concept and validation plan.

Develop system performance specification and system validation plan.

Expand performance specification into configuration items "Design-to" specifications and verification plan.

Evolve "Design-to" specifications into "Build-to" documentation and inspection plan.

Fab, assemble, and code to "Build-to" documentation

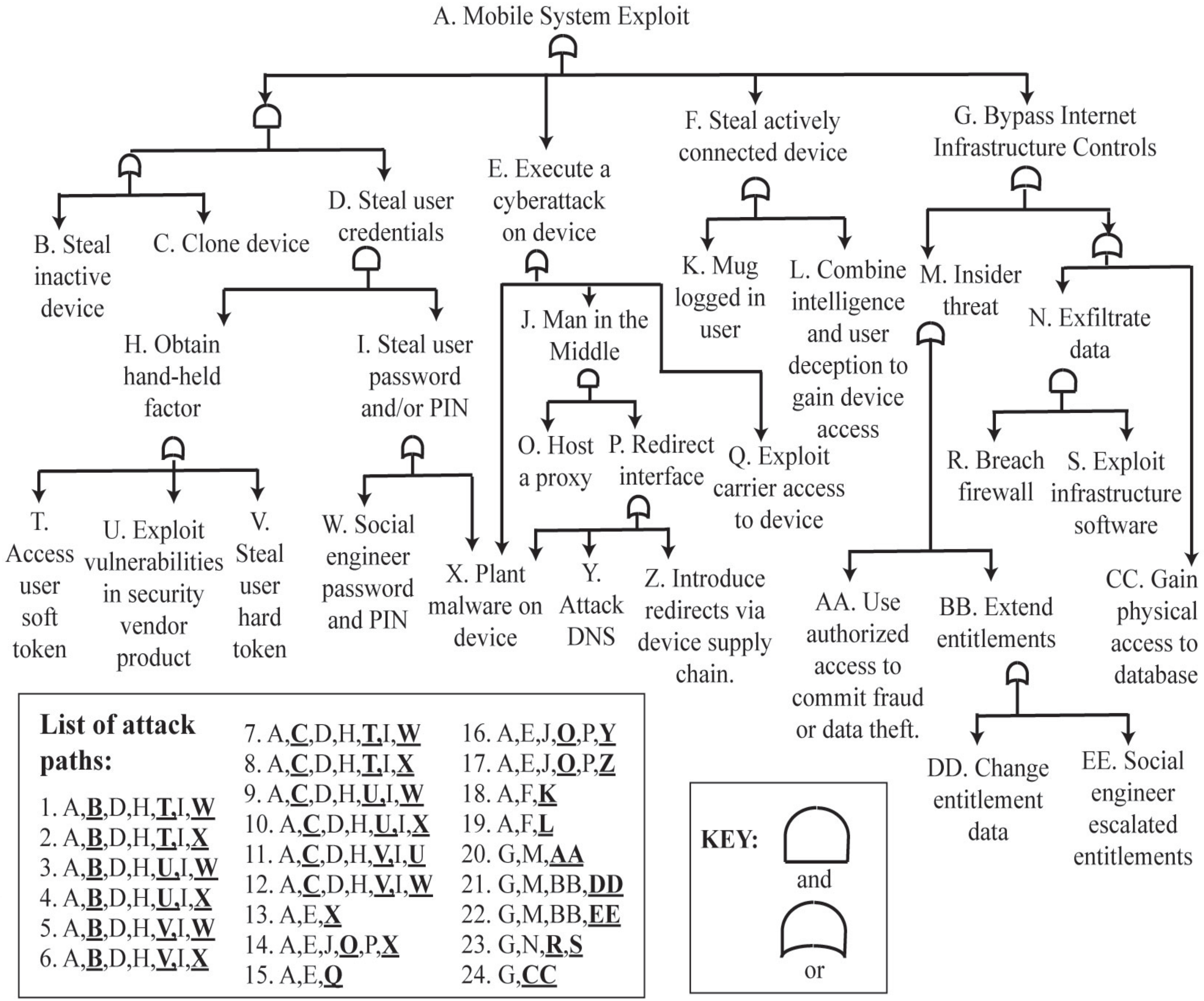
Inspect "Build-to" documentation.

Assemble configuration items and perform item verification to item "Design-to" specifications.

Integrate system and perform system verification to performance specification.

Demonstrate and validate system to user validation plan.

Design Basis Threat


A. Mobile System Exploit
B. Steal inactive device
C. Clone device
D. Steal user credentials
E. Execute a cyberattack on device
F. Steal actively connected device
G. Bypass Internet Infrastructure Controls
H. Obtain hand-held factor
I. Steal user password and/or PIN
J. Man in the Middle
K. Mug logged in user
L. Combine intelligence and user deception to gain device access
M. Insider threat
N. Exfiltrate data
O. Host a proxy
P. Redirect interface
Q. Exploit carrier access to device
R. Breach firewall
S. Exploit infrastructure software
T. Access user soft token
U. Exploit vulnerabilities in security vendor product
V. Steal user hard token
W. Social engineer password and PIN
X. Plant malware on device
Y. Attack DNS
Z. Introduce redirects via device supply chain.
AA. Use authorized access to commit fraud or data theft.
BB. Extend entitlements
CC. Gain physical access to database
DD. Change entitlement data
EE. Social engineer escalated entitlements
KEY:
and
or

List of attack paths:

1. A,**B**,D,H,**T**,I,**W**
2. A,**B**,D,H,**T**,I,**X**
3. A,**B**,D,H,**U**,I,**W**
4. A,**B**,D,H,**U**,I,**X**
5. A,**B**,D,H,**V**,I,**W**
6. A,**B**,D,H,**V**,I,**X**
7. A,**C**,D,H,**T**,I,**W**
8. A,**C**,D,H,**T**,I,**X**
9. A,**C**,D,H,**U**,I,**W**
10. A,**C**,D,H,**U**,I,**X**
11. A,**C**,D,H,**V**,I,**U**
12. A,**C**,D,H,**V**,I,**W**
13. A,E,**X**
14. A,E,J,**O**,P,**X**
15. A,E,**Q**
16. A,E,J,**O**,P,**Y**
17. A,E,J,**O**,P,**Z**
18. A,F,**K**
19. A,F,**L**
20. G,M,**AA**
21. G,M,BB,**DD**
22. G,M,BB,**EE**
23. G,N,**R**,**S**
24. G,**CC**

Validation Example: SWFR

A SWFR is a product of two measurements, defined as:

- The time to protect (TTP), the average interval between when a target is first aware of the existence of a new threat and when it successfully deflects it, will depend on the controls preventing exploit on that path, and is measured as the minimum time required to establish compensating or corrective controls.
- The time to attack (TTA), measured as the median lifetime of malicious activity emanating from a specific source, is the length of time that an attack is available to the attacker would be calculated for each leaf activity
- For every path P on an attack tree, calculate SWFR of P, then:

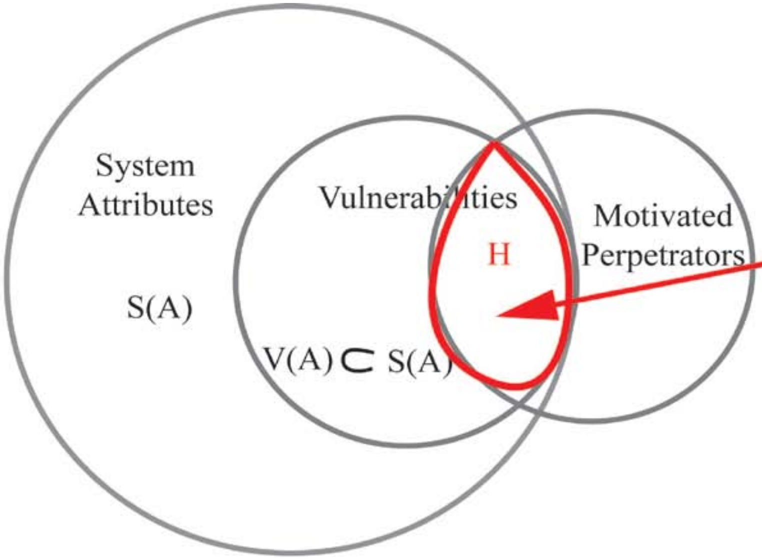
  System SWFR = max ($P_{1SWFR} \ldots P_{nSWFR}$)

- To the extent the ratio TTP/TTA is minimized, the defenders are successfully thwarting attacks. To the extent it increases, the attackers are more successful. The goal of absolute security would be measured with a TTP/TTA metric that is better as the ratio approached zero.

Comparing Security Validation Metrics

Adversary Activity	Metrics	Process 1	Process 2
Disable infrastructure	TTP (in hours)	2	4
	TTA = 24 hours	24	24
	SWFR	.8	.16
Subvert control system	TTP (in days)	12	24
	TTA = 120 days	120	120
	SWFR	.1	.2

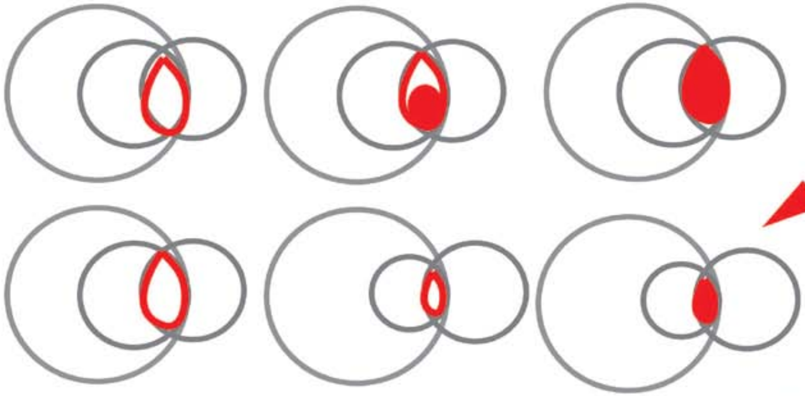
Graphical Illustration of the System Level Approach



Target for
Thwarting Attributes
such as:
Compensating Controls
OR
System Attribute Redesign

Traditional iterative security architecture review

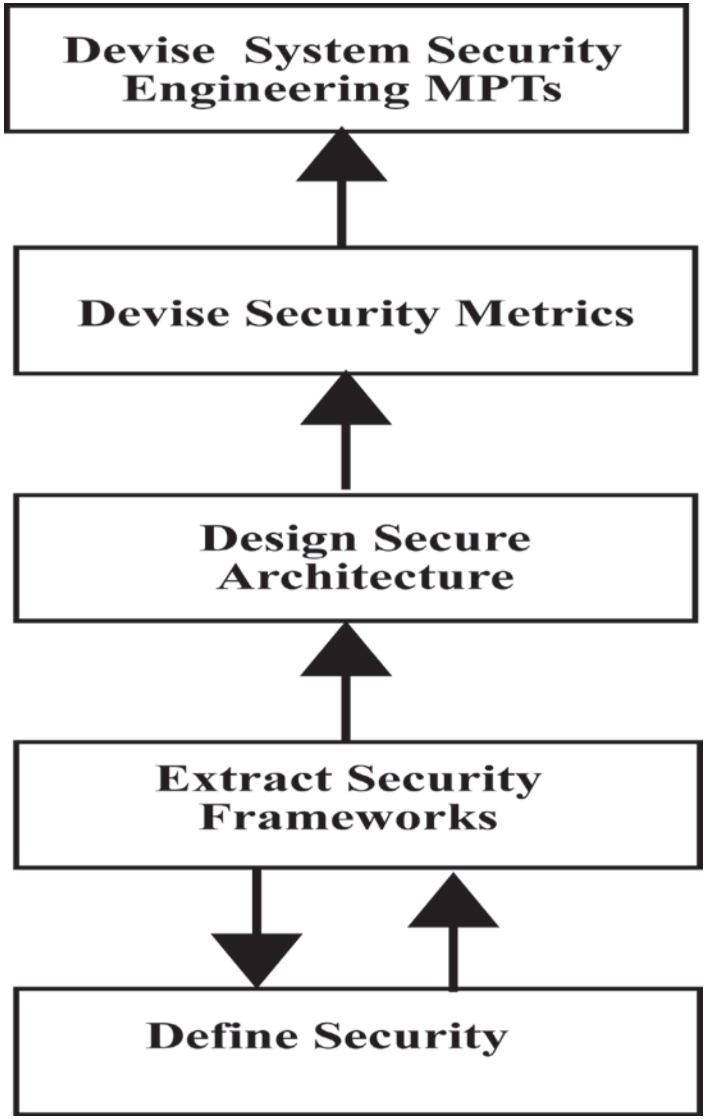
versus security architecture framework



Change in systems attributes reduces requirements for compensating controls

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

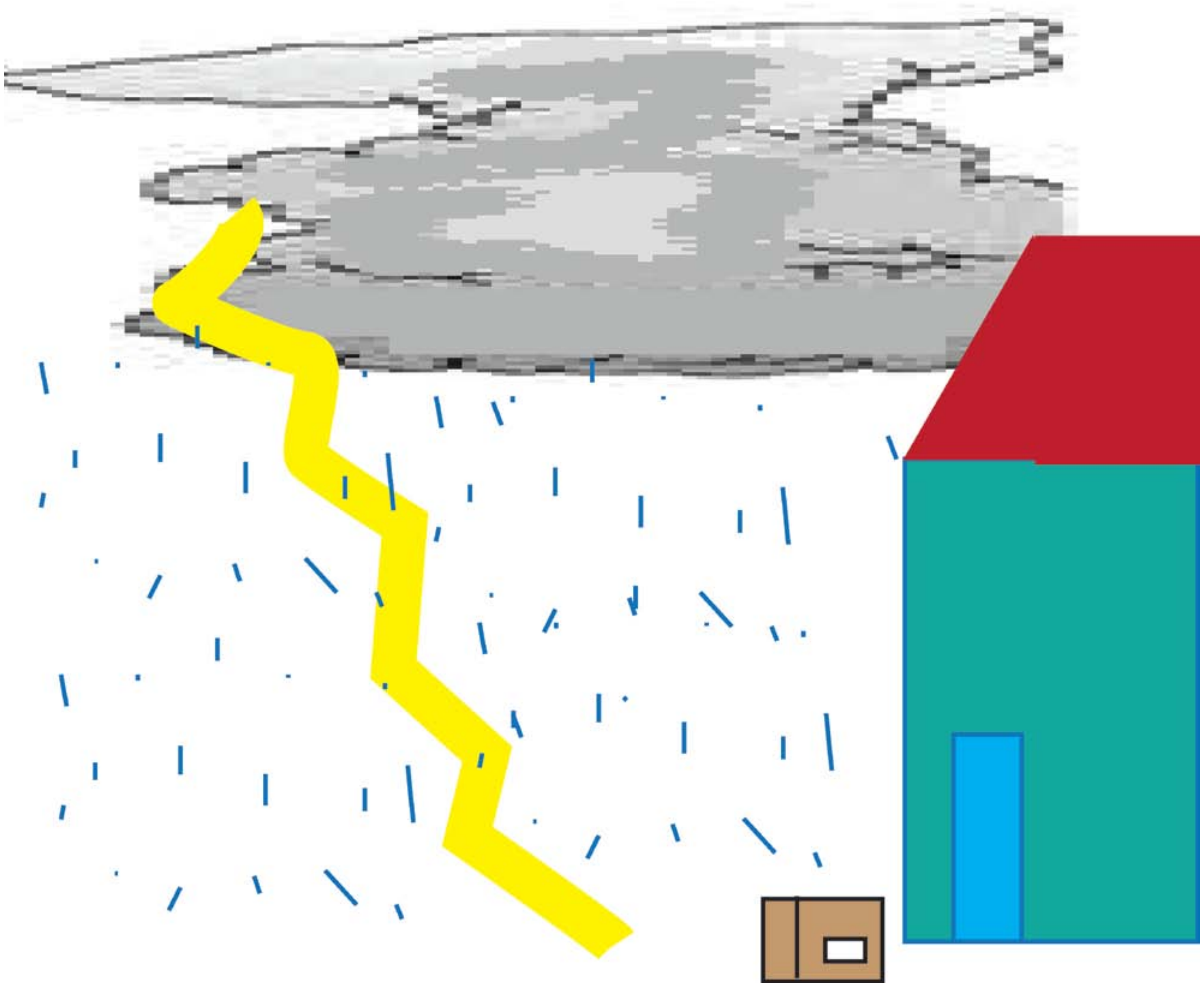
Systems Security Methodology


Devise System Security Engineering MPTs
Devise Security Metrics
Design Secure Architecture
Extract Security Frameworks
Define Security

SYSTEMS ENGINEERING
Research Center

www.sercuarc.org

Weatherproofing Analogy



Questions, Discussion?

jennifer@bayuk.com

www.bayuk.com