Security and Assurance Architectures

Ricardo Villalón

Security Architecture Description

Security Architecture Description

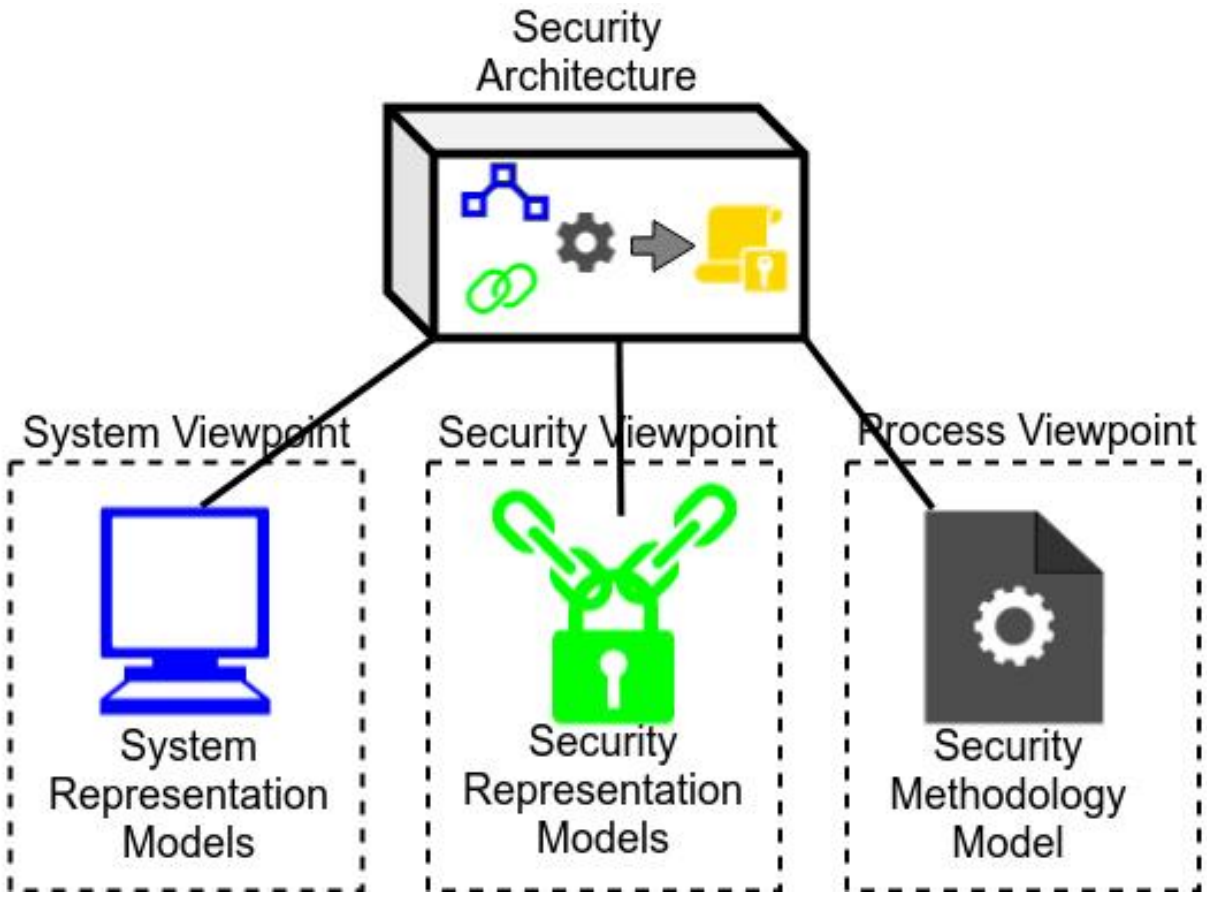
Based on ISO/IEC/IEEE 42010

Stakeholders: consumers, developers, technical working group, evaluators, security officers, auditors, architects, designers, accreditors.

Concerns: how to consider organization security policies, threats, vulnerabilities, more security properties, security objectives for TOE and OE, system global security, automation of security, different system sizes and complexity, security governance

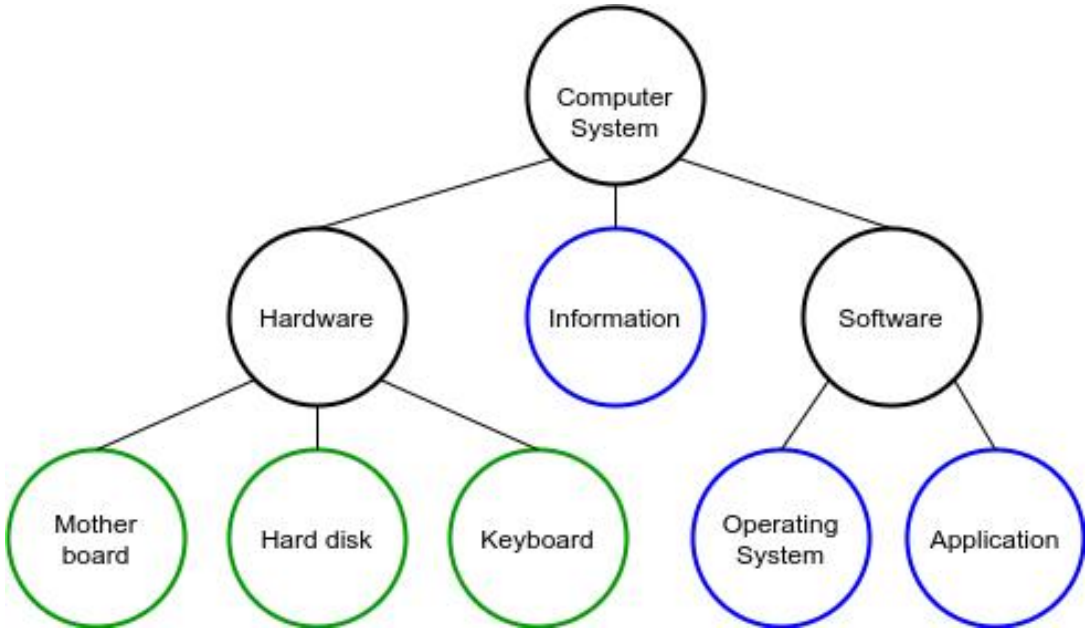
Viewpoints: system, security, process.

Models: system representation, security representation, security methodology.

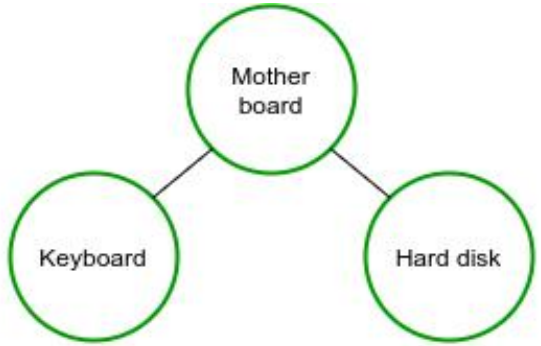


System Representation

Representing system structure
Whole-parts diagrams



Representing system functions/capabilities
Interaction diagrams



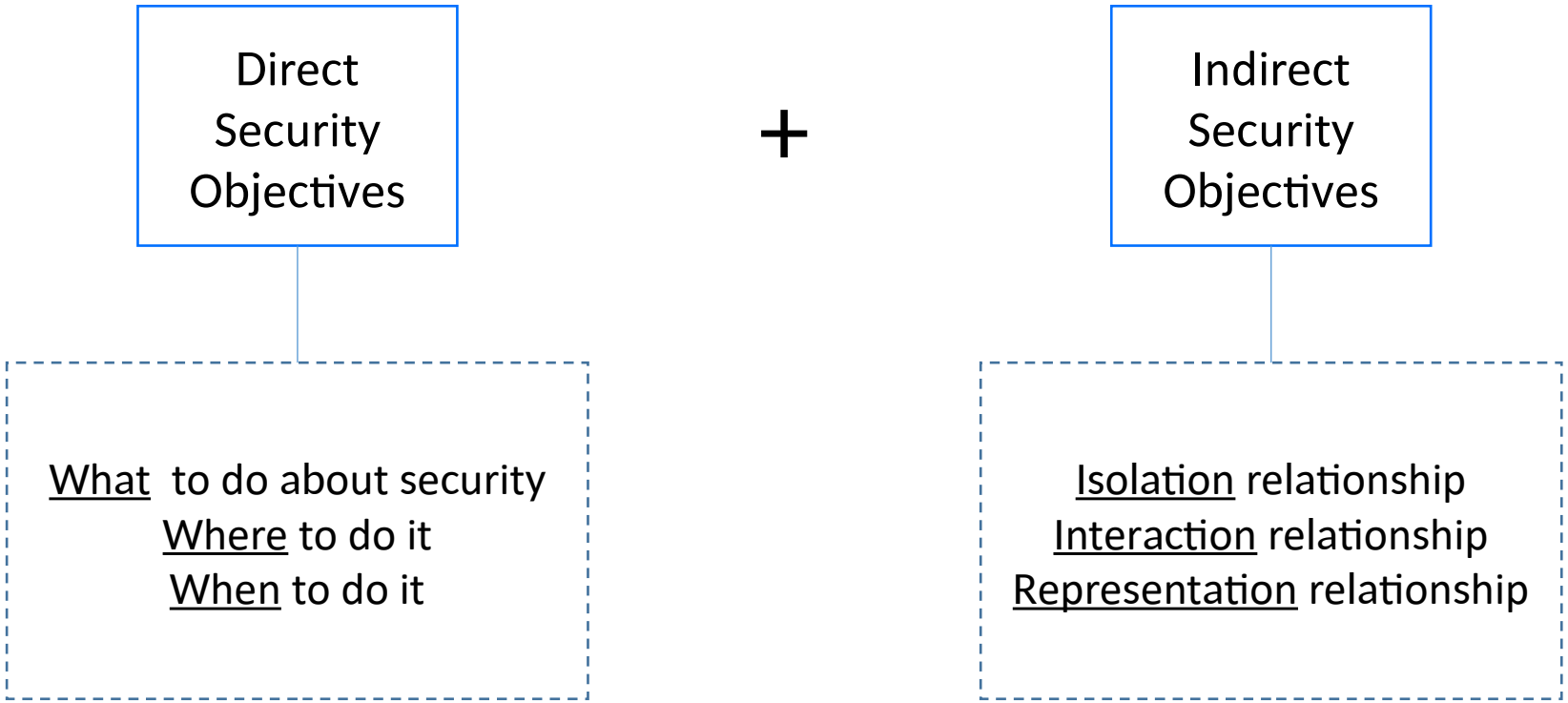
Physical Interaction

Digital Interaction

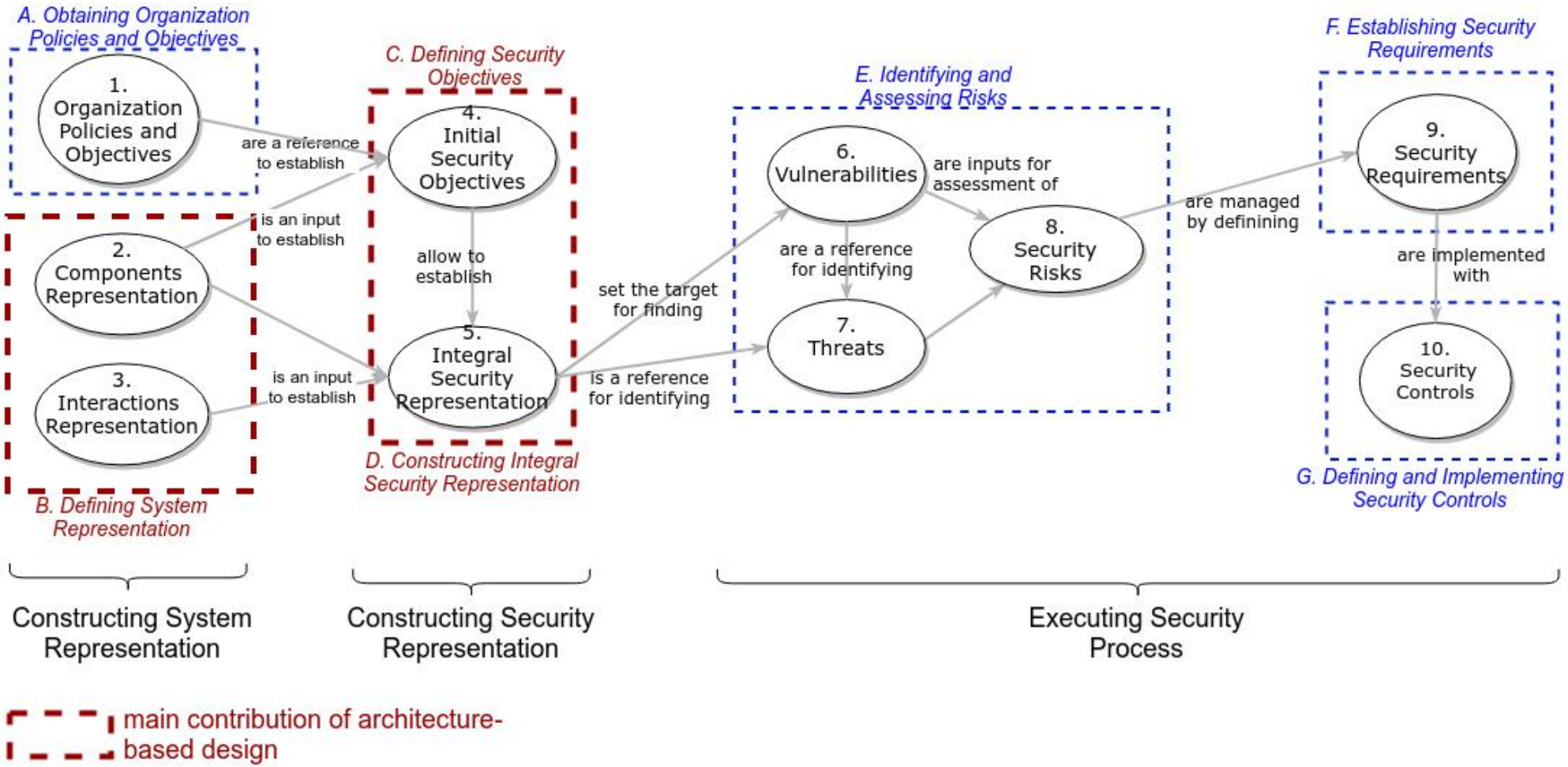
Security Representation

Direct security objectives: describing the main (initial) security goals

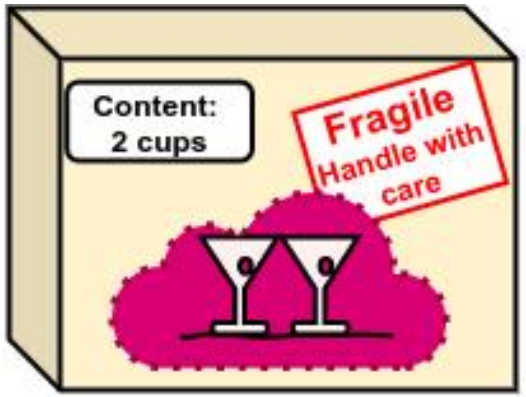
Indirect security objectives: can be found when security relationships are identified



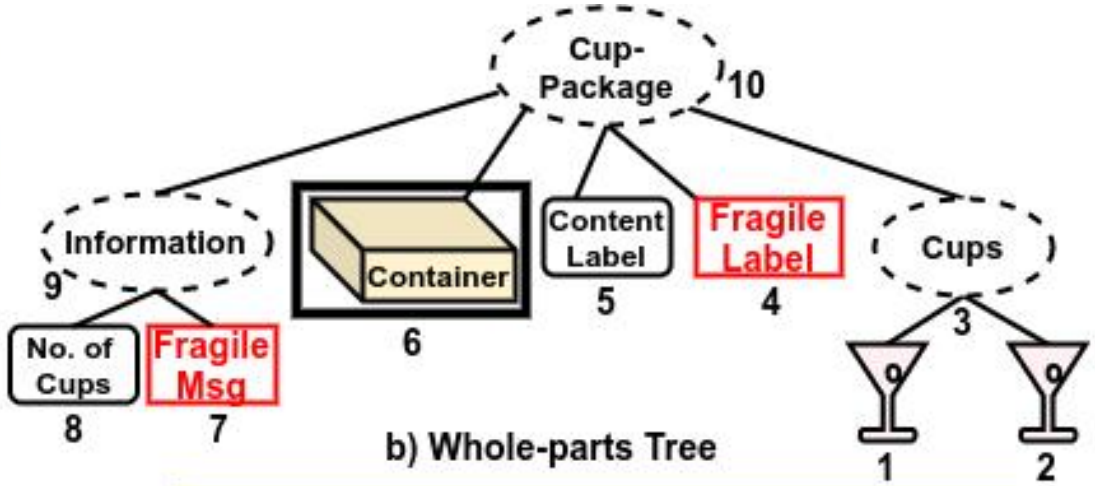
Security Methodology Proposal



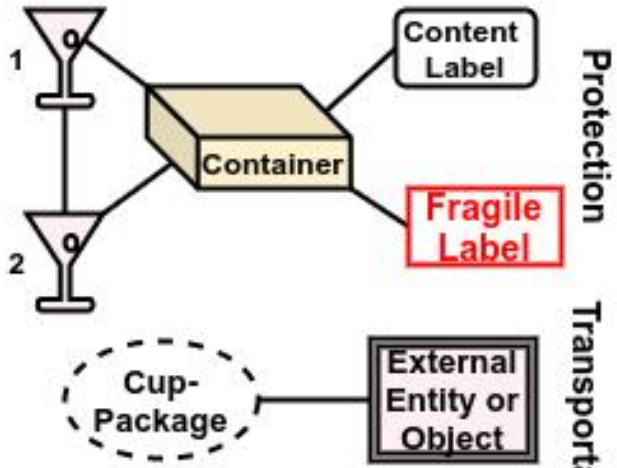
Cup Package Example



a) Cup-Package System



b) Whole-parts Tree



c) Interaction Diagrams

Component 1	Component 2	Representation
Cups	No. of Cups	Size of Cups
No. of Cups	Content Label	Physical Representation
Cup1, Cup 2	Fragile Msg	Fragility of Cup 1 and Cup 2
Fragile Msg	Fragile Label	Physical Representation

d) Representation Relationship Table

Cup Package Security Objectives

We want to prevent the cups from being broken or lost while transported to their destination

DO[1][1] *We want to prevent the Cup 1 from being broken while transported to its destination.*

DO[1][2] *We want to prevent the Cup 1 from being lost while transported to its destination.*

DO[2][1] *We want to prevent the Cup 2 from being broken while transported to its destination.*

DO[2][2] *We want to prevent the Cup 2 from being lost while transported to its destination.*

DO[3][1] *We want to prevent the Cups from being broken while transported to their destination.*

DO[3][2] *We want to prevent the Cups from being lost while transported to their destination.*

DO[10][1] *We want to prevent the Cup-Package from being broken while transported to its destination.*

DO[10][2] *We want to prevent the Cup-Package from being lost while transported to its destination.*

Assurance Architecture Description

Assurance Architecture Description

Based on ISO/IEC/IEEE 42010

Stakeholders: consumers, developers, technical working group, evaluators, security officers, auditors, architects, designers, accreditors.

Concerns: Threats to security and organizational security policy commitments clearly articulated and the security controls be demonstrably sufficient. Measures to reduce the likelihood of vulnerabilities, the ability to exercise them, and the extent of the damage. Measures to facilitate subsequent identification elimination, mitigation, and/or notification of exploited or triggered vulnerabilities.

Viewpoints: security solution, evaluation, process.

Model kinds: system representation, evaluation representation, assurance methodology.