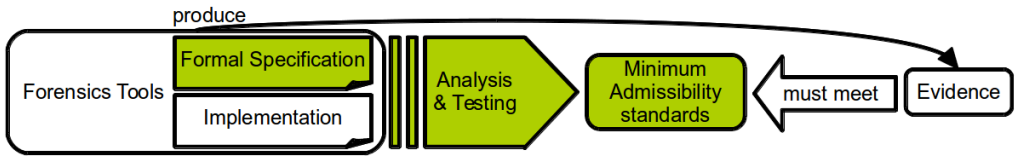
A Formal Model for Forensic Storage Media Preparation Tools

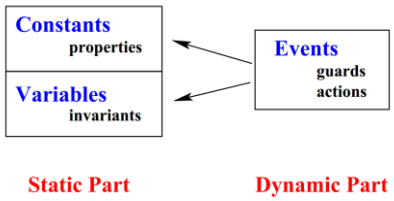
Benjamin Aziz
benjamin.aziz@port.ac.uk
School of Computing, University of Portsmouth, United Kingdom

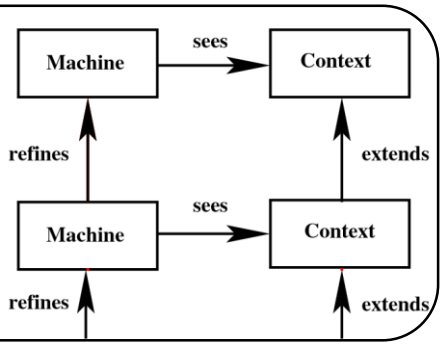
Philippe Massonet, Christophe Ponsard
{philippe.massonet,christophe.ponsard}@cetic.be
CETIC, Charleroi Belgium

Problem statement



Event-B formal language





CONTEXT ForensicsStorageMedia
SETS
Data
CONSTANTS
benignDataElement
AXIOMS
axm3 : Data≠∅
axm2 : benignDataElement∈Data
END

MACHINE VisibleSectors **SEES** ForensicsStorageMedia
VARIABLES
ForensicStorageMedium
Terminated // *machine terminated or not*
INVARIANTS
inv1 : ForensicStorageMedium ⊆ Data
inv2 : Terminated ∈ BOOL
Terminated = TRUE ⇒
Completeness : **∀x·(x ∈ ForensicStorageMedium) ⇒ (x = benignDataElement))**
EVENTS
Preparation ≙
ANY
visibleSector
benignDataSet
WHERE
grd1 : Terminated = FALSE
grd2 : visibleSector ⊆ ForensicStorageMedium
grd3 : ∀x·(x ∈ visibleSector) ⇒ (x ≠ benignDataElement)
grd4 : visibleSector ≠ ∅
grd5 : ∀x·(x ∈ benignDataSet) ⇒ (x = benignDataElement)
grd6 : card(benignDataSet) = card(visibleSector)
THEN
act1 : ForensicStorageMedium ≔ ((ForensicStorageMedium\visibleSector) ∪ benignDataSet)
END

MACHINE WithHiddenSectors **REFINES** VisibleSectors
VARIABLES
ForensicStorageMediumHiddenAreas
overwriteHiddenData // *support overwriting hidden areas*
INVARIANTS
inv1 : ForensicStorageMediumHiddenAreas ⊆ Data
inv2 : overwriteHiddenData ∈ BOOL
EVENTS
HiddenSectorPreparation ≙
ANY
hiddenSector
benignDataSet
WHERE
grd7 : Terminated = FALSE
grd8 : hiddenSector ⊆ ForensicStorageMediumHiddenAreas
grd9 : ∀x·(x ∈ hiddenSector) ⇒ (x ≠ benignDataElement)
grd10 : hiddenSector ≠ ∅
grd11 : ∀x·(x ∈ benignDataSet ⇒ (x = benignDataElement)
grd12 : card(benignDataSet) = card(hiddenSector)
grd13 : overwriteHiddenData = TRUE
THEN
act11 : ForensicStorageMediumHiddenAreas ≔ ((ForensicStorageMediumHiddenAreas \hiddenSector) ∪ benignDataSet)
END

Discussion: a formal reference modelling using a refinement approach (using Event-B here) enables

1. the progressive injection of details into the model as needed by the system and context (including threats) e.g. an additional third level can be introduced for the Erase hardware command in the prepared device.
2. specific proofs to be established w.r.t. tool (design) properties such as **correctness** but also **completeness** however **accuracy** could not be specified or reasoned on in a uniform manner

Key References: Abrial, J.-R. (2010). Modeling in Event-B: System and Software Design. Cambridge University Press
Casey, E. and Rose, C. (2010). Forensic Discovery: Handbook of Digital Forensics and Investigation. Academic Press.
Gladyshev, P. and Enbacka, A. (2007). Rigorous Development of Automated Inconsistency Checks for Digital Evidence Using the B Method. International Journal of Digital Evidence, 6(2).
NIST (2009). Forensic storage media preparation tool specification (v1.0). Technical report, NIST

Work supported by the Evidence FP7 project (nr 608185). Thanks to Yoann Guyot for helping in the poster design.