Possibilistic Information Flow Control for Workflow Management Systems

Thomas Bauereiss
Dieter Hutter

DFKI Bremen

Universität Bremen

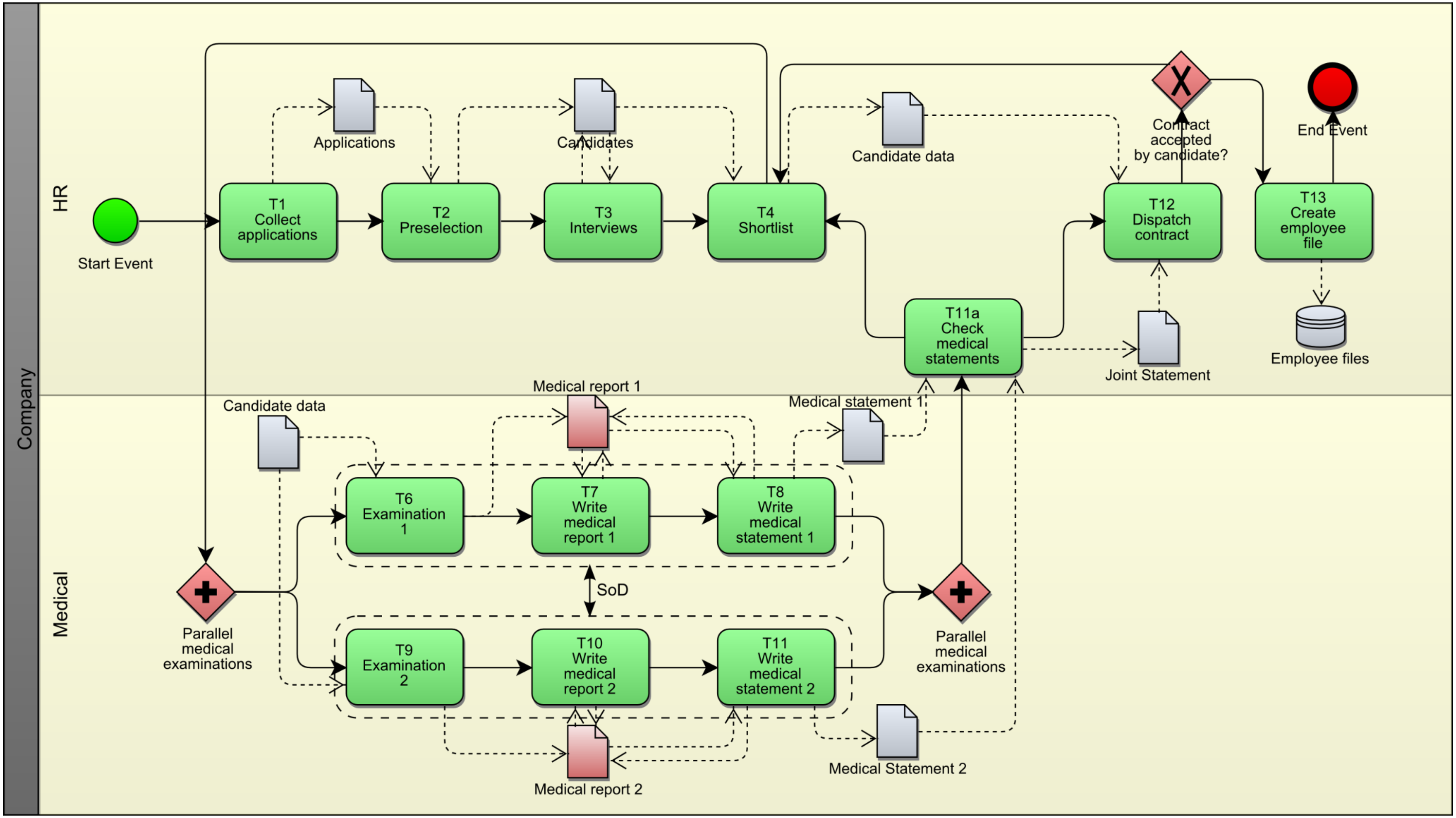
Workflow management systems

- Coordinating manual and (semi-)automatic activities involving multiple users

- Security requirements on data, e.g. confidentiality
  - Example: Participants without a need to know must not learn about contents of a document

- Security requirements on the process, e.g. separation of duty
  - Example: Decision must be approved independently by a different person

Workflow management systems



Information flow control

- Explicit data flows typically prevented via access control (e.g. Wolter et al (2009) map security annotations to XACML policies)

- Implicit flows of information via observation of system, e.g.
  - Control flow depends on confidential data
  - Observation of progress of workflow
    → Deductions about value of confidential data possible

- (Possibilistic) information flow control
  - Confidential events must not interfere with visible system behaviour

Related work

- Previous work on information flow in workflow systems
  - Accorsi, R., Lehmann, A.: Automatic information flow analysis of business process models. In: BPM. LNCS, vol. 7481, pp. 172–187. Springer (2012)
  - Yang, P., Lu, S., Gofman, M.I., Yang, Z.: Information flow analysis of scientific workflows. Journal of Computer and System Sciences 76(6), 390–402 (Sep 2010)

- Room for improvement
  - Support larger class of (semantic) notions of information flow security
  - Explicitly consider interplay with other security requirements

Overview

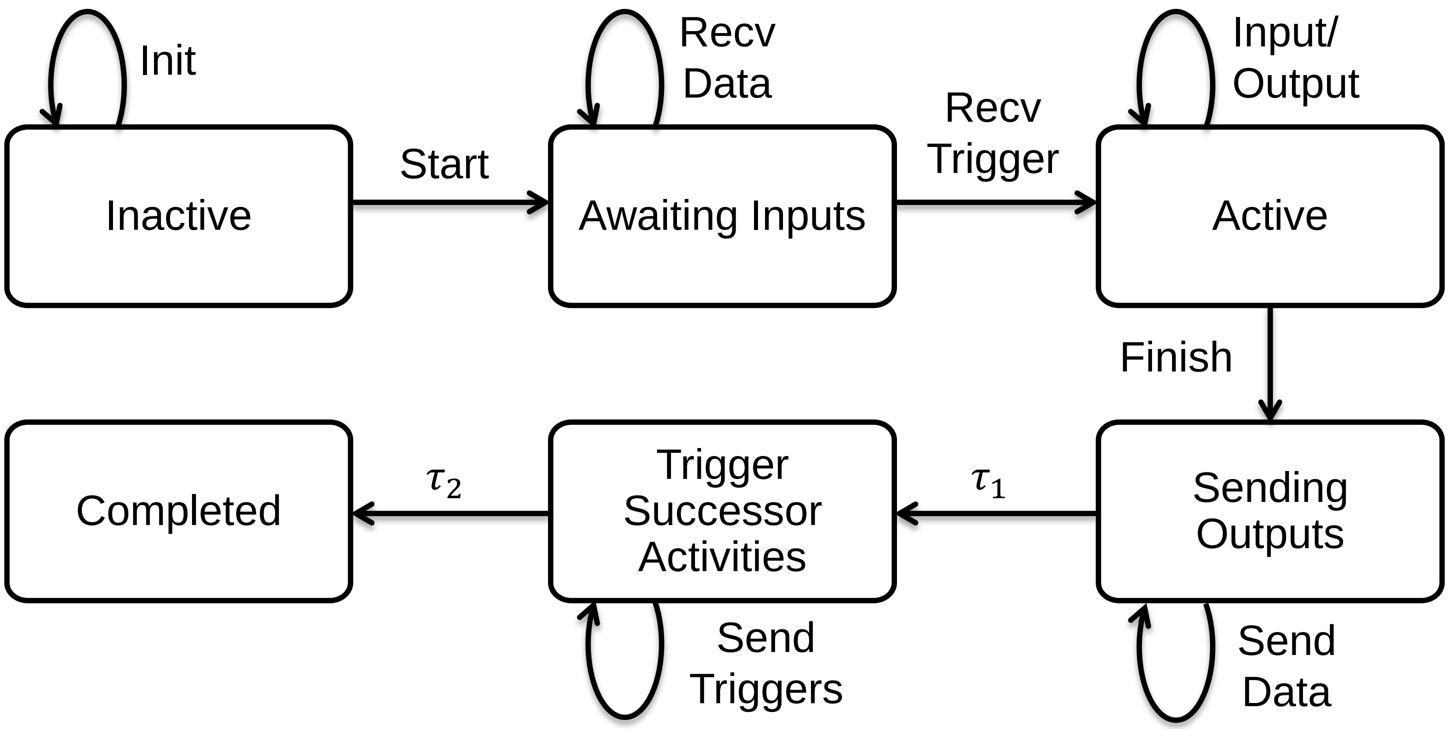
- Formal semantics of
  - workflows in terms of state-event systems, and
  - security annotations in terms of IFC and SoD
- Verification approach for IFC
  - Application of methodology for compositional verification (Hutter et al, 2007)
  - Unwinding proofs for simple example activities
- Sufficient conditions for compatibility of IFC and SoD

System model

- Each activity in the workflow modelled as a state-event system
- Overall workflow system: Composition of activities + communication platform
- Allows modelling of
  - Internal data processing
  - Sequence flows and data associations between activities
    - Captures basic subset of BPMN
    - Extended features remain future work (cf. other proposals for formal semantics of BPMN, e.g. Wong & Gibbons)

System model

- Each activity in the workflow modelled as a state-event system



Separation of duty

- Two tasks constrained by SoD have to be performed by two different persons, e.g.
  - Medical examinations by two different medical officers
  - Loan to be approved by different person than the one who requested it (fraud prevention)

- Can be modelled as safety property (i.e. predicate on individual traces)
  - $P = \{\tau \mid \forall e, e' \in \tau. (e \in E_1 \wedge e' \in E_2) \longrightarrow user(e) \neq user(e')\}$

Confidentiality of documents

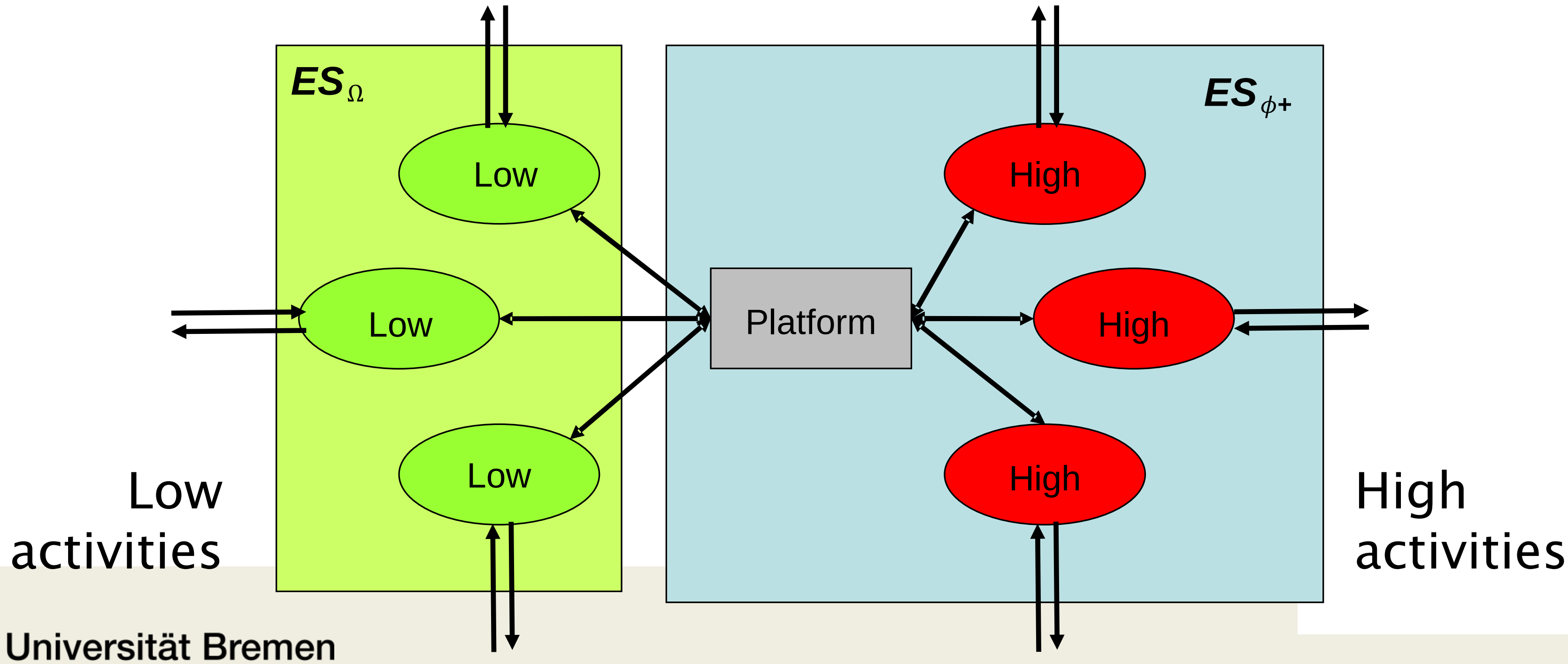
- Security policy
  - Set of security domains (e.g. HR, Medical)
  - Flow policy: (Transitive) relation on domains
  - Domain assignment for data items, activities, users

- Security view $\mathcal{V} = (V, N, C)$ for each domain:
  - V = events of visible activities (e.g. all HR activities)
  - C = I/O containing confidential data (e.g. medical reports)

- Security predicate, e.g.
  - $BSD_{\mathcal{V}}(Tr) \equiv \forall \alpha, \beta \in E^*. \forall c \in C. (\beta . c . \alpha \in Tr \wedge \alpha|_C = \langle\,\rangle)$
    $\Rightarrow \exists \alpha' \in E^*. (\beta . \alpha' \in Tr \wedge \alpha'|_C = \langle\,\rangle \wedge \alpha'|_V = \alpha|_V)$

Compositional verification of IFC

- Application of decomposition methodology [HMSS07]
- Verification of individual activities wrt. suitable local views implies security of composed system wrt. global view
- Increases scalability, facilitates reuse of proofs



Verification of activity agents

- C-preserving local view for each activity a, e.g.
  - globally confidential events are locally confidential,
  - communication events with low activities are visible,
  - consistency between local views, e.g. $Send_a(b, m) \in V_a$ iff $Recv_b(a, m) \in V_b$
- Proof using unwinding technique for MAKS predicates
  - Reduces conditions on whole traces to more local conditions on transitions of the system
  - Example: Observations possible in the post-state of a confidential transition are also possible in the pre-state

Verification of activity agents

- Sufficient conditions for security of example activities
  - User I/O activities (if access control is enforced)
  - Gateways for deciding on control flow (if decision does not depend on confidential data)
- Proofs split into reusable part (wrapper) and activity-specific behaviors (that can be plugged into the wrapper)
- Proofs verified in Isabelle using I-MAKS formalization developed at TU Darmstadt

Compatibility of SoD and IFC

- Issue: Enforcing a safety property can violate possibilistic information flow security
- Example:
  - Anonymity requirement vs.
  - SoD between a confidential and a visible activity
  - ➢ Leak: Information who has *not* participated in the confidential activity
- Sufficient conditions for compatibility of SoD and IFC
  - events in $E_1 \cup E_2$ are all confidential/non-confidential, or
  - user assignment events are non-confidential

Summary

- Specification of security requirements on both data and processes using MAKS predicates / safety properties
- Formal model of workflow systems as composition of state event systems
- Adaptation and integration of existing techniques for compositional verification
- Current results verified in Isabelle/HOL based on existing formalisation of MAKS framework

Future work

- Theory
  - Refinement, i.e. propagation of security properties between abstract and concrete level, switch to language-based techniques
  - Controlled declassification, i.e. specify what an attacker may deduce and when

- Practice
  - Tool support, e.g. automatic translation of annotated BPMN diagrams to Isabelle, proof automation
  - Evaluation in a realistic application scenario, e.g. conference management system

References

[BH14] Bauereiss, T. & Hutter, D. Compatibility of Safety Properties and Possibilistic Information Flow Security in MAKS. IFIP SEC2014, Springer, 2014 (to appear)

[GM82] Goguen, J. & Meseguer, J. Security policies and security models. IEEE Symposium on Security and Privacy, 1982, 11

[HMSS07] Hutter, D.; Mantel, H.; Schaefer, I. & Schairer, A. Security of multi-agent systems: A case study on comparison shopping. J. Applied Logic, 2007, 5

[M00] Mantel, H. Possibilistic Definitions of Security - An Assembly Kit. CSFW, IEEE Computer Society, 2000, 185-199

[M02] Mantel, H. On the Composition of Secure Systems. IEEE Symposium on Security and Privacy, IEEE Computer Society, 2002, 88-101

[SS09] Seehusen, F. & Stolen, K. Information flow security, abstraction and composition. IET Information Security, 2009, 3, 9-33

[WG08] Wong, P. Y. H. & Gibbons, J. A Process Semantics for BPMN. ICFEM, Springer, 2008, 5256, 355-374

[WMS+09] Wolter, C.; Menzel, M.; Schaad, A.; Miseldine, P. & Meinel, C. Model-driven business process security requirement specification. Journal of Systems Architecture, 2009, 55, 211-223

[ZL97] Zakinthinos, A. & Lee, E. S. A General Theory of Security Properties. IEEE Symposium on Security and Privacy, IEEE Computer Society, 1997, 94-102