BlueSky: Activity Control: A Vision for "Active" Security Models for Smart Collaborative Systems

Tanjila Mawla
Department of Computer Science
Tennessee Tech University

Maanak Gupta
Department of Computer Science
Tennessee Tech University

Ravi Sandhu
Institute for Cyber Security (ICS) and NSF C-SPECC Center,
University of Texas at San Antonio

ACM Symposium on Access Control Models and Technologies

June 8 - 10th, 2022

Activity -Centric Access Control

- The notion of Activity
- Authorization (A)
- Obligations (B)
- Conditions (C)
- Dependencies among Activities (D)

Comparison Overview of Features Proposed in ACAC Model

Table 1: Comparison Overview of Features Proposed in ACAC Model with other related models.

Models	Notion of Activity	Multiple Object Activities	Activities Concur-rency	Activity Precedence	Activities Depen-dency	Incompatible Activities	Conditional Constraints	Activities Mutability	Run-time Authoriza-tion	Obligations
TBAC	Yes	No	Yes	No	No	No	No	No	Yes	No
UCON	No	No	No	No	No	No	Yes	No	Yes	Yes
ACON	Yes	No	No	No	No	No	Yes	No	No	No
ABAC	No	No	No	No	No	No	Yes	No	No	No
ACAC	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES

FOUNDATIONS OF ACTIVITY-CENTRIC MODEL FOR COLLABORATIVE ECOSYSTEM

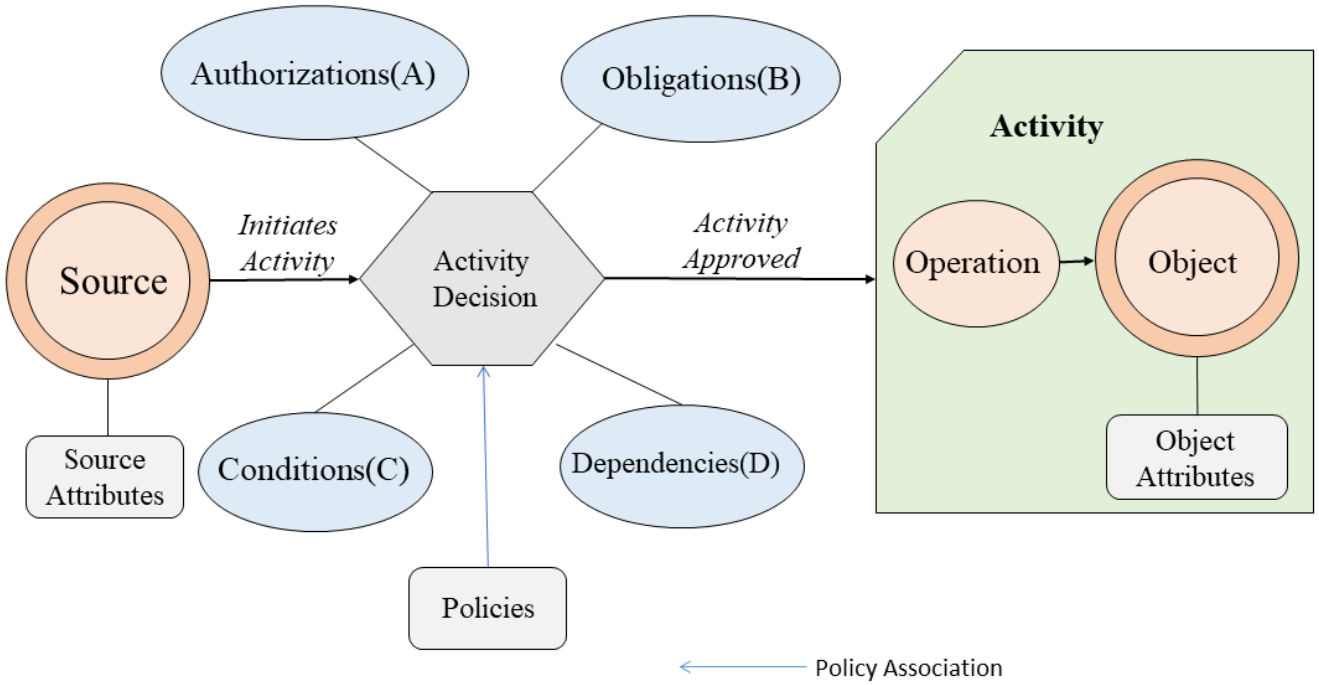

Figure 1: ACAC Model Components.

FOUNDATIONS OF ACTIVITY-CENTRIC MODEL FOR COLLABORATIVE ECOSYSTEM (Cont.)

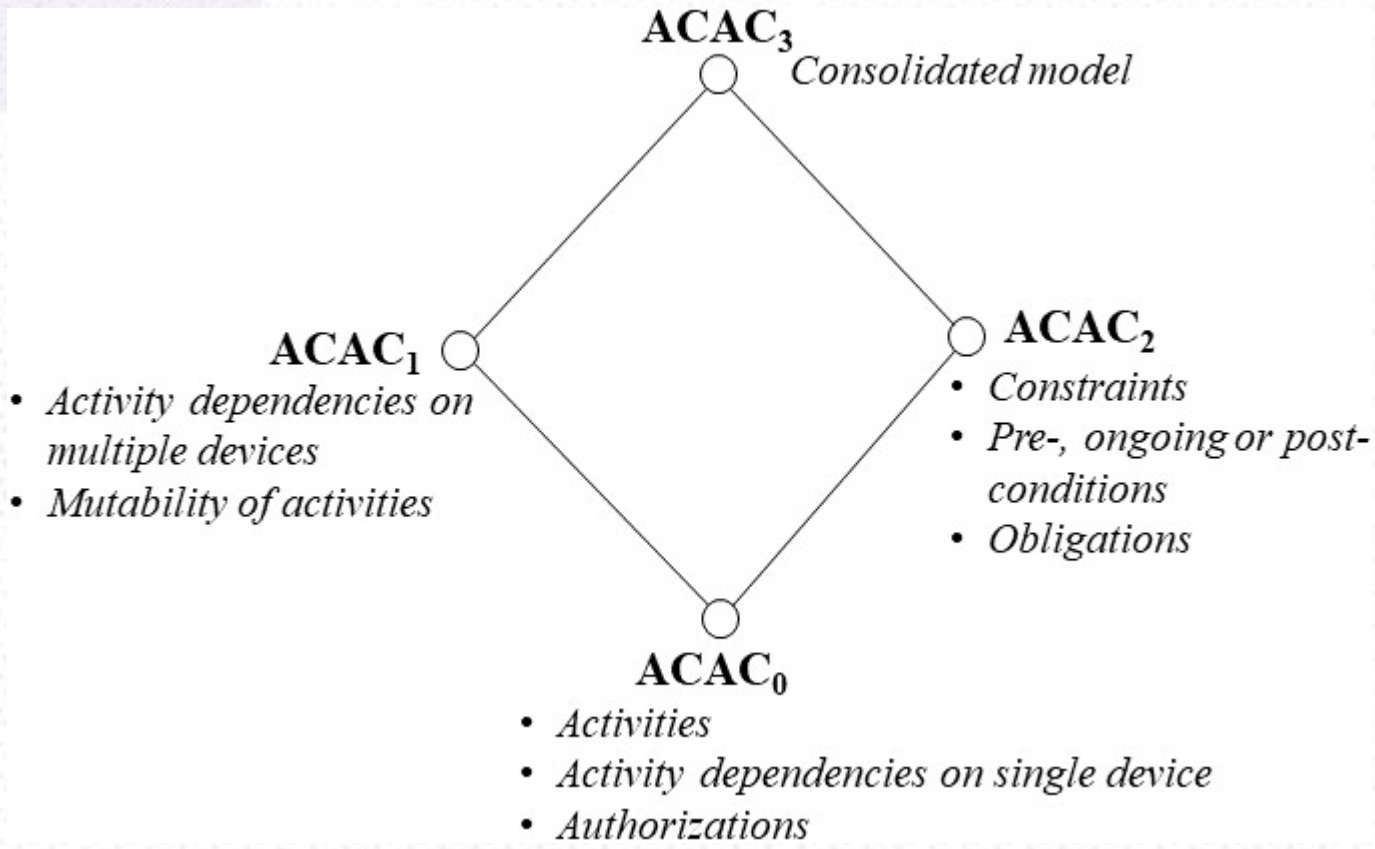

Figure 2: A Framework for a Hierarchy of ACAC models

FOUNDATIONS OF ACTIVITY-CENTRIC MODEL FOR COLLABORATIVE ECOSYSTEM (Cont.)

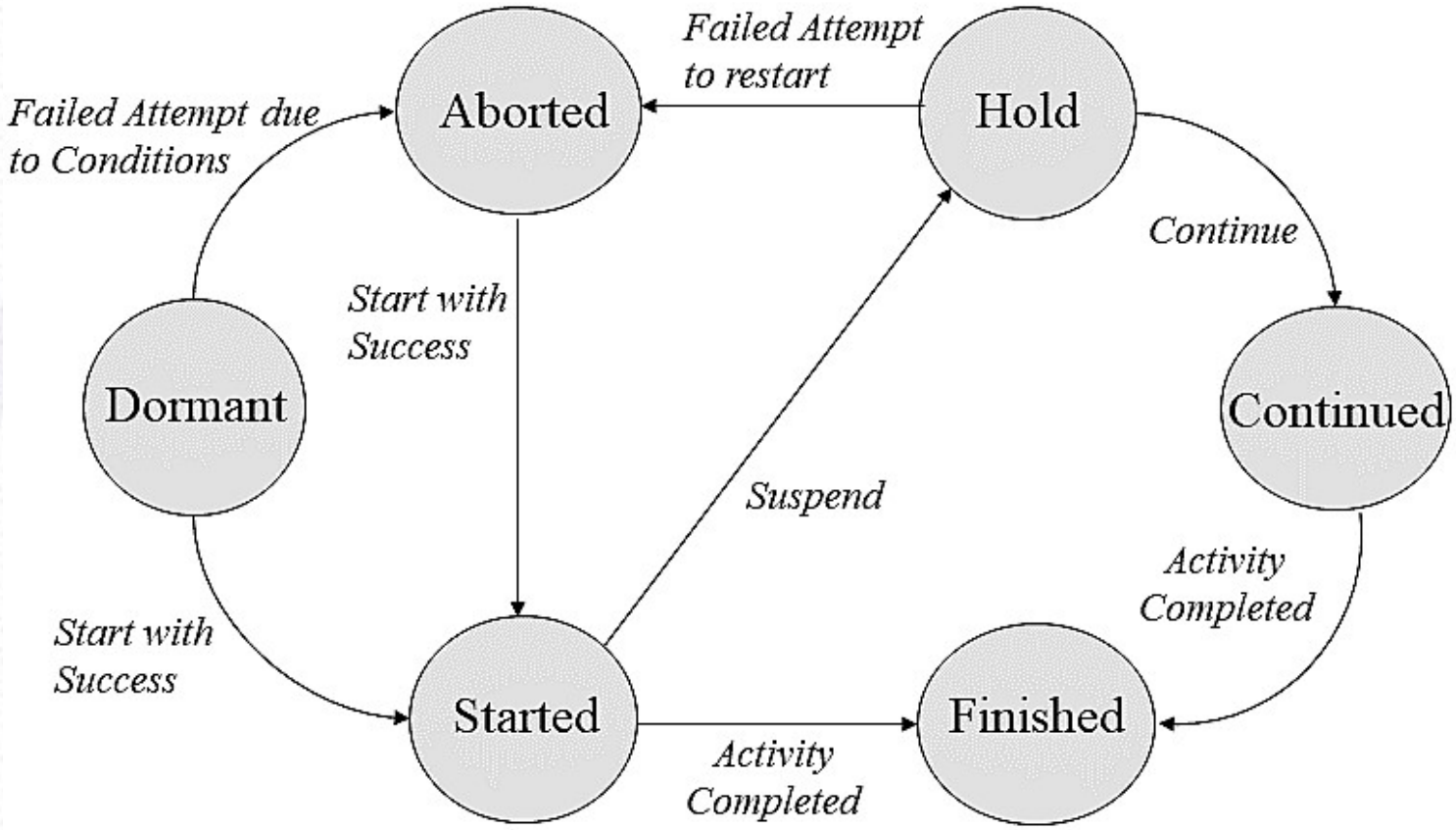

Figure 3: States of an Activity

FOUNDATIONS OF ACTIVITY-CENTRIC MODEL FOR COLLABORATIVE ECOSYSTEM (Cont.)

Table 2: Mutability of Dependent Activities in terms of the invocation time related to a requested activity. √ and × respectively denote the presence (mandatory or optional) and absence of the corresponding field to support the relationships in the first column

Activities Relation-ship	Immutable	Pre-invocation	Parallel invoca-tion	Post-invocation
Independent	√	√	√	√
Ordered	×	√	×	√
Concurrent	×	×	√	×
Temporary	×	√	√	√
Precedence	×	×	×	√
Conditional	×	√	√	√
Incompatible	×	×	×	×

ACAC and Zero-Trust

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy —including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

Future Research Agenda

- Operational and administrative formal model.
- Policy language and enforcement architecture.
- Risk adaptive ACAC incorporating zero-trust tenets.
- Self-adaptive and AI-driven ACAC Deployment

Selected References

- Thomas, R.K. and Sandhu, R.S., 1998. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In *Database security XI* (pp. 166-181). Springer, Boston, MA.

- Park, J. and Sandhu, R., 2004. The UCONABC usage control model. *ACM transactions on information and system security (TISSEC), 7*(1), pp.128-174.

- Park, J., Sandhu, R. and Cheng, Y., 2011, August. Acon: Activity-centric access control for social computing. In *2011 Sixth International Conference on Availability, Reliability and Security* (pp. 242-247). IEEE.

- Jin, X., Krishnan, R. and Sandhu, R., 2012, July. A unified attribute-based access control model covering DAC, MAC and RBAC. In *IFIP Annual Conference on Data and Applications Security and Privacy* (pp. 41-55). Springer, Berlin, Heidelberg.

- Gupta, M. and Sandhu, R., 2021, June. Towards activity-centric access control for smart collaborative ecosystems. In *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies* (pp. 155-164).

- Rose, S., Borchert, O., Mitchell, S. and Connelly, S., 2020. Zero trust architecture (No. NIST Special Publication (SP) 800-207). National Institute of Standards and Technology.

Thank You!

Questions?