Multi-Party Access Control: Requirements, State of the Art and Open Challenges

Anna Cinzia Squicciarini
Pennsylvania State University
asquicciarini@ist.psu.edu

Sarah Michele Rajtmajer
Quantitative Scientific Solutions
sarah.rajtmajer@qs-2.com

Nicola Zannone
Eindhoven University of Technology
n.zannone@tue.nl

ABSTRACT

Multi-party access control is gaining attention and prominence within the community, as access control models and systems are faced with complex, jointly-owned and jointly-managed content. Traditional single-user approaches lack the richness and flexibility to accommodate these scenarios, resulting in undesired disclosure of sensitive data and resources. Moving forward fundamental work in this area is critical. In particular, as personal data amasses and algorithms for data mining improve, personally identifiable information is more readily inferred and the practical implications of privacy decisions are relatively opaque. This is true even at the individual level, but the parallel problem for jointly managed content involves the cross product of these complex outcomes. In this presentation, we discuss fundamental requirements of successful multi-party access control mechanisms and contextualize these concepts with respect to the state of the art. Based on this analysis, we identify open challenges and draw a roadmap for future work.

CCS CONCEPTS

• **Security and privacy → Access control**; • **Human-centered computing → Collaborative and social computing systems and tools**;

KEYWORDS

Collaborative access control; data governance; literature study.

ACM Reference Format:
Anna Cinzia Squicciarini, Sarah Michele Rajtmajer, and Nicola Zannone. 2018. Multi-Party Access Control: Requirements, State of the Art and Open Challenges. In *SACMAT '18: The 23rd ACM Symposium on Access Control Models & Technologies (SACMAT), June 13–15, 2018, Indianapolis, IN, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3205977.3205999

1 SUMMARY

In the highly connected networks typifying today's online communities, the sharing of content attributable to multiple owners or stakeholders is increasingly frequent. Users need to make collaborative decisions about content-sharing, while adequate multi-party decision mechanisms are not yet in place.

Traditional, single-user access control policies currently supported by main-stream services and collaborative environments are insufficient for jointly-managed content in important ways. They focus on confidentiality rather than facilitating controlled sharing. Access decisions are often binary, or based on inflexible policies. This inflexibility can inhibit mission-critical information sharing, e.g., in hospitals, intelligence departments, fire departments, and the military – organizations that commonly handle and protect sensitive, private data, but also rely on sharing that data appropriately.

Furthermore, single-user driven policies make it difficult, if not impossible, to determine whether a given disclosure meets the privacy expectations of all involved parties, and as such threaten to violate the expectations of both content owners and stakeholders. Along these lines, the impacts of collaborative decision making on users' behaviors and dynamic user interactions are largely unexplored. In particular, we have yet to understand how individuals' sharing decisions change over time, who are the most influential users, how they benefit from it, and the privacy gains and losses from a collective perspective.

This current gap in research may be the result of several (related) causes. To our knowledge, proposed content sharing models to date have not been translated into practical features or applications, as social networks provide minimal support for joint decision-making scenarios. Hence, an exploration in the wild of the effects of multi-party sharing is fundamentally hard. In addition, work to date on multi-party sharing has adopted a micro-scale view of the interactions among users (i.e., one-on-one and one-shot interactions), in an attempt to minimize discomfort and other security properties one interaction at a time. However, it is possible that group dynamics at the collective scale are distinct from the aggregation of one-on-one interactions between members within the group. While literature on collective behavior abounds, these considerations have yet to find their place within the discourse of multi-party access control.

In this presentation, we outline what we believe to be plausible steps forward for the research community to address community-centric access control. We discuss fundamental requirements of developed solutions with respect to policy specification, governance, usability and transparency, and we contextualize these requirements within the state of the art. We discuss both state of the science as well as the state of practice, with direct comparison of existing methods, their capabilities and limitations. We identify open challenges, and in doing so, aim to provide a roadmap of key points for future work in the community. This presentation is based on [1].

Acknowledgement Work from Dr. Squicciarini is partly funded by NSF Grant 1453080. Work from Dr. Zannone is partially funded by the ITEA projects M2MGrids (13011) and APPSTACLE (15017).

REFERENCES

[1] Federica Paci, Anna Squicciarini, and Nicola Zannone. 2018. Survey on Access Control for Community-Centered Collaborative Systems. *ACM Comput. Surv.* 51, 1, Article 6 (2018), 38 pages. https://doi.org/10.1145/3146025

SACMAT '18, June 13–15, 2018, Indianapolis, IN, USA

ACM ISBN 978-1-4503-5666-4/18/06.
https://doi.org/10.1145/3205977.3205999