How soon can you decide whether Alice is permitted to communicate or share resources with Bob?

Bernard Butler and Brendan Jennings
TSSG, Waterford Institute of Technology, Ireland
{bbutler,bjennings}@ieee.org

ABSTRACT

Organisations are deploying ever more complex communications and content management systems to control entitlements to read, write and share protected digital resources. The resulting access control policy infrastructure defines and resolves the complex decision boundary between *safety* and *openness*. Moreover, for information security models enabling *ethical wall* policies, the decision boundary itself can change dynamically. This complexity poses major usability concerns in real-time corporate communication scenarios (due to high complexity) and in online social networks (due to large scale).

Researchers continue to propose improvements designed to increase policy evaluation performance. These proposals include reconfiguration of policies (reordering, regrouping and combining) and re-implementation of Policy Decision Points (PDPs) to, for example, use binary decision diagrams for evaluation [1]. Other proposals include novel policy languages with lightweight data formats commonly utilised in highly scalable web systems. Griffin et al. [2] describes such an implementation, evaluated using a flexible testbed that collects PDP service times and enables principled statistical comparison of access control performance improvement proposals.

As discussed by Papakonstantinou et al. [3], access control performance is also a problem when protecting semantically rich, highly-distributed linked data. The authors describe how reasoning and query rewriting techniques in that domain can be fully integrated with data access operations. Our initial findings when applying these ideas to rich domain models of communication in large enterprises suggest this integrated approach has benefits for fine-grained access control policy evaluation performance.

BODY

Guaranteeing access control policy evaluation performance is hard. Results from scalable web systems and semantic analysis show promise.

REFERENCES

[1] S. Pina Ros, M. Lischka, and F. Gómez Mármol. Graph-based XACML Evaluation. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT 2012)*, pages 83-92, ACM, 2012.

[2] L. Griffin, B. Butler, E. de Leastar, B. Jennings, and D. Botvich. On the Performance of Access Control Policy Evaluation. In *Proceedings of the 13th IEEE International Symposium on Policies for Distributed Systems and Networks (Policy 2012)*, pages 25-32, IEEE, 2012.

[3] V. Papakonstantinou, M. Michou, I. Fundulaki, G. Flouris, and G. Antoniou. Access Control for RDF Graphs using Abstract Models. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies (SACMAT 2012)*, pages 103-112, ACM, 2012.

Volume 2 of Tiny Transactions on Computer Science