OXFORD UNIVERSITY COMPUTING LABORATORY

research in

Models and Technologies for Secure Data Sharing

UNIVERSITY OF OXFORD

Andrew Simpson, David Power, Douglas Russell, and Mark Slaymaker

"Existing legal and technical mechanisms intended to protect our privacy, copyright, and other important values have been overwhelmed by the increasingly open information environment in which we live… We face the real risk that the technical laws spelled out by Gordon Moore (growth in processing power) and Robert Metcalfe (network effects) will permanently overwhelm our values as enshrined in society's laws."

D. J. Weitzner et al.,
Information Accountability.
Communications of the ACM 51(6):82–87,
June 2008

Increasing amounts of data are being collected on all of us in our roles as citizens, consumers and patients. While it is certainly the case that there is a wealth of relevant legislation and guidelines to determine how personal data might be used, it is typically the case that there is a significant disconnect between the 'high level' rules that govern such use and the 'low level' enforcement of those rules. It is also typically the case that in any but the simplest of cases, it is difficult to characterise precisely "who can see what". Our concern is the development of models and technologies to help facilitate appropriate and assured data sharing: *appropriate* in the sense that policies conform to high-level requirements; *assured* in the sense that we have confidence in such assertions.

sif

sif (service-oriented interoperability framework) is a lightweight security and data integration layer based on Java and web services. The framework facilitates the secure aggregation of data from heterogeneous data sources. Originally developed to support the secure sharing of healthcare data, it now supports a variety of applications in which organisations wish either to integrate disparate legacy systems or to transfer data securely in a point-to-point fashion.

Evolving access control

Our mechanism for evolving access control allows the expression and enforcement of authorisation policies that may change dynamically on the basis of observed events, such as, for example, audited actions. This gives rise to policies of the form "Jim can access table A or table B, but not both" or "Andrew can't access anything that Jeremy has accessed". The evolving access control mechanism can be used either to facilitate secure access to a single database or in conjunction with sif to provide dynamic access control within distributed contexts.

The application of lightweight formal models

Clearly, the problem of "who can see what" becomes more difficult when an authorisation mechanism can change access policies automatically without reference to a systems administrator. Through abstract, formal models we are able to construct and explore mathematical representations of such dynamic policies prior to deployment.

Some recent publications

M. A. Slaymaker, D. J. Power, D. Russell, and A. C. Simpson. *On the facilitation of fine-grained access to distributed healthcare data*. In the Proceedings of Secure Data Management 2008, pages 169—184. Springer-Verlag Lecture Notes in Computer Science, volume 5159, 2008.

D. J. Power, M. A. Slaymaker, and A. C. Simpson. *On the construction and verification of self-modifying access control policies*. In the Proceedings of Secure Data Management 2009, pages 107—121. Springer-Verlag Lecture Notes in Computer Science, volume 5776, 2009.

M. A. Slaymaker, D. J. Power, and A. C. Simpson. *Formalising and validating RBAC-to-XACML translation using lightweight formal methods*. In Proceedings of ABZ 2010, pages 349—362. Springer-Verlag Lecture Notes in Computer Science, volume 5977, 2010.

A. C. Simpson, D. J. Power, D. Russell, M. A. Slaymaker, V. Bailey, C. E. Tromans, J. M. Brady, and L. Tarassenko. *GIMI: the past, the present, and the future*. To appear in the Philosophical Transactions of the Royal Society A, 2010.

For further information contact:

Dr Andrew Simpson
Oxford University Computing Laboratory
Wolfson Buiding
Parks Road
Oxford OX1 3QD

Andrew.Simpson@comlab.ox.ac.uk
ph: +44 1865 283514
fx: +44 1865 283531

or see the web site at:

www.comlab.ox.ac.uk/activities/securedatasharing