Institution: University of Kent

Unit of Assessment: 11: Computer Science

Title of case study: PERMIS – A modular authorisation infrastructure

1. Summary of the impact

PERMIS is a suite of open source security software, written mostly in Java, which provides an application-independent, standards-based, authorisation infrastructure that enables software developers to incorporate state of the art authorisation functionality into their systems with a minimum of effort.

PERMIS has been integrated into a wide variety of environments including grids, clouds and more specialised domains, leading to more secure systems for end users at a reduced cost of implementation; for example, the Swiss Ministry of Defence has adapted PERMIS for use in an air force application. It consistently gets more than 1000 downloads per year, with over 100 new users registering annually.

2. Underpinning research

PERMIS was the first implementation of the 2001 ISO/ITU-T X.509 standard for a privilege management infrastructure (PMI). Chadwick is the UK BSI representative to ISO/ITU-T X.509 meetings, and since 2001 he has edited the PMI sections of the X.509 standard, incorporating several of the features of the PERMIS implementation into the standard. More recently support for other security standards has been included in PERMIS, including OASIS SAML tokens (these are used by Shibboleth in the UK Access Management Federation) and OASIS XACML request contexts and obligations.

Although the original PERMIS research was funded under the EC ISIS programme (Jan 2001 – Sept 2002), the majority of the R&D has taken place since 2005, at Kent. Since 2005 Chadwick (Kent 2004-present) has attracted over £1.5m to Kent in PERMIS related grants, many of them in collaboration with other partners. The overriding theme in this work has been how to develop an easy to use, application-independent, authorisation infrastructure with sophisticated access control features, which can be used in distributed environments such as grids, clouds and federations, so that authorisation is uniformly enforced throughout. Since 2005, over a dozen RAs and PhDs have been involved in this research at Kent, including: Bailey, Casenove, Fatema, Ferdous, Ferreira, Hibbert, Inman, Laborde, Lievens, Nasser, Nguyen, Otenko, Shi, Su, Siu, Xu, and Zhao. All have been successfully employed after graduation.

The key underpinning research contributions can be classified under 5 themes:

A. Usability - how to allow users and administrators to easily write their authorisation policies in controlled natural language (EPSRC, joint with Prof. Sasse, UCL and EC FW 7 project (TAS3), joint with 14 other partners). [1,4: references here refer to the publications listed in section 3]
B. Application of well-known physical security capabilities to electronic authorisation systems - how to implement Separation of Duties in a federated system where there is no central control over role assignment (JISC joint with CLRCC); how to introduce Break the Glass functionality into RBAC systems, so that users can override 'deny' decisions in emergency situations (EC FP7 -TAS3). [4]
C. Development of novel electronic authorisation features - first to design and implement privacy preserving attribute aggregation in federated identity management systems (JISC funded), to add "sticky policies" to a distributed application independent authorisation infrastructure (EC FP7 -TAS3), and to coordinate authorisation decision making throughout a distributed system such as a grid (EPSRC, joint with Prof Basden, Salford). [3,4,5]
D. Integrating security standards - how to integrate a PMI into SAML/Shibboleth (JISC funded) and first to show how NIST Levels of Assurance can be integrated into authorisation decision

making (JISC, joint with Manchester).[4]
E. Integration with grid/cloud computing - How to integrate a policy based authorisation infrastructure into Grids, in particular to Globus Toolkit v4 (JISC funded), how to provide cloud services with a privacy protecting authorisation infrastructure that allows a resource owner to *grant anyone access to any of his cloud resources at any time* (EPSRC funded) and how to define and build an architecture and set of Open APIs for federated access to and sticky policy use in the OpenStack open source cloud implementation (EPSRC, joint with Cranfield). [2,4,6]

3. References to the research [**- 4,5,6 best reflect the quality of the underpinning research]

Note that the 4 references for Chadwick in REF2 relate to the underpinning research above.

1. P Inglesant, MA Sasse, D Chadwick, LL Shi *Expressions of expertness: the virtuous circle of natural language for access control policy specification* ". 4th Symposium On Usable Privacy and Security (SOUPS), July 23-25, 2008, Pittsburgh, PA. BEST PAPER AWARD (24 cites in Google Scholar).
2. RO Sinnott, DW Chadwick, T Doherty, D Martin, A Stell, G Stewart, L Su, J Watt *Advanced security for virtual organizations: The pros and cons of centralized vs decentralized security models*, Proc. 8th IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2008). (37 cites in Google Scholar).
3. David W Chadwick, Linying Su, Romain Laborde. "*Coordinating Access Control in Grid Services*". Concurrency and Computation: Practice and Experience, Volume 20, Issue 9, Pages 1071-1094, June 2008. (15 cites in Google Scholar).
4. **David Chadwick, Gansen Zhao, Sassa Otenko, Romain Laborde, Linying Su and Tuan Anh Nguyen. "*PERMIS: a modular authorization infrastructure*". Concurrency And Computation: Practice And Experience. Volume 20, Issue 11, Pages 1341-1357, August 2008. (Listed in REF2) (58 cites in Google Scholar).
5. **David W. Chadwick, George Inman. "*Attribute Aggregation in Federated Identity Management*". IEEE Computer, May 2009, pp 46-53 (31 cites in Google Scholar).
6. **David W Chadwick, Kaniz Fatema. "*A Privacy Preserving Authorisation System for the Cloud*". Journal of Computer and System Sciences, vol 78, Issue 5, Sept 2012. pp 1359–1373 (listed in REF2). (4 cites in Google Scholar)

Funding for this research. All grants have Chadwick as PI.

i) My Private Cloud. March 2011-July 2011. £50k. EPSRC
ii) Trusted Architecture for Securely Shared Services (TAS3). EC. Jan 2008-Dec 2011. €1,051k (€9.5M total)
iii) Integrating VOMS and PERMIS for Superior Secure Grid Management (VPMan). JISC. March 2007-July 2008. £85k
iv) Shib-Grid Integrated Authorization (Shintau). JISC. March 2007-March 2009. £183k
v) Easy Expression of Authorisation Policies. EPSRC. Sept 2006-April 2008.£113k
vi) Participation in Grid Standards, EPSRC GridNet 2 grant. £12.5k July 2005-Dec 2007
vii) A Grid Authorisation API v2, JISC £43K, Oct 2005-June 2008

4. Details of the impact

With funding from UK and EC sources we have turned our research results into open source code that has been exploited in multiple different sectors. The objective of the PERMIS research has been to deliver proof of concept privilege management infrastructure (PMI) software for the software engineering community to experiment with, build into their prototype applications, and if desired, re-engineer into commercial or military grade products. In this way we achieve the highest possible impact for the lowest cost.

The strategy has been very successful, and we have had 475 registrations from Jan 2008 to July 2013, excluding all Kent users. Software downloads have consistently been in the thousands per year, and between Aug 2009 and July 2013 totalled nearly 14,000 (excluding Kent). An analysis of

the geographic spread, taken from the IP addresses of the top 20 downloaders in 2012, shows the global reach of the impact: 6 from China; 2 from India, 2 from Taiwan, 5 from the USA, and 1 each from Vietnam, Rumania, France, Israel, and the UK. (Note that a username and password are needed so they are not accessible by web crawlers.)

As can be seen, the PERMIS software is being used globally, but being security related, information about how PERMIS is being used and by whom is kept confidential by most users, who provide pseudonyms when registering for downloads. Gmail, yahoo, 163 and hotmail email addresses are most commonly used. They invariably do not respond when asked for details about how they are using PERMIS. However some users do identify their organisations, and over the years registrations have been recorded from Alcatel-Lucent, JMP Chase, Deloitte, South African Government, Siemens, Thales, Adobe, Booz Allan and Orange. One major project that used PERMIS was the €41million FI-Ware project (see http://www.fi-ppp.eu/projects/fi-ware/). This is a consortium of all the major European Telecom providers, whose goal is to *"advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees*."

From personal contacts and visits Chadwick knows that PERMIS has been used for several years by a large multinational aerospace, defence and security company (who wish to remain anonymous) in their research labs. Initially the PERMIS authorisation decision engine was used for authorisation decision making, and more recently the Delegation Issuing Service has been integrated into many security use cases. Their objective is to provide industry-ready solutions focused on role management and authorization.

From email correspondence, Chadwick knows that a US based leading provider of management consulting, technology, and engineering services is evaluating the use of PERMIS as an alternative Policy Decision Point to be used in an environment where standards based web services can be rapidly built and deployed. No further details can be released due to the sensitivity of the work.

Among the companies that are using PERMIS and are happy to share the experience, we can report examples from the following domains: telecoms, defence, virtualisation, audit:

Unizeto Technologies SA, Poland, [S4: references are to contacts listed in Section 5] is working with the Polish Ministry of Economy and Ministry of Justice in order to issue PERMIS X.509 AC's to either individuals or companies, confirming that they have either private economic activity
https://prod.ceidg.gov.pl/CEIDG/ceidg.public.ui/Search.aspx
or are established and registered in the national registry
https://ems.ms.gov.pl/krs/wyszukiwaniepodmiotu
The objective is to build a policy based authorisation system built on AC's issued by the government.

The Toyota National College of Technology, Japan [S1] is using PERMIS to provide RBAC access to its high security hypervisor called BitVisor. The initial development of BitVisor was initiated by the National Information Security Center of Japan in 2009. In the initial development, Dr. Hirano designed the ID management functions of BitVisor which required the user to have a smartcard with an X.509 certificate before he can access a PC, but the PC was statically configured. Adding PERMIS to Bitvisor allows the administrator to dynamically configure the use of BitVisor on PCs. Dr Manabu Hirano from Toyota came as a visiting researcher to work with Prof Chadwick from June 2012 to Jan 2013, in order to perform the design and integration research. BitVisor is currently being commercialised by IGEL, a Japanese SME.

The Swiss Ministry of Defence [S3] has especially rigorous security standards and therefore need military grade software. Consequently it has hardened the core components of PERMIS for use in an air force application. It released the code back to the community as Hardened PERMIS, originally via the EC OSOR web site - no longer available, but the archive version is here:
http://web.archive.org/web/20111113084114/http://www.osor.eu/projects/openpermis
which kept statistics about its code base. It reported that:

"The estimated cost to develop this project is 1,810,915 EUROS This project has 74,854 lines of code. To develop a similar application you would need 18.58 person-years."

When the OSOR web site merged into the EC joinup web site in 2011, Hardened PERMIS was moved to *https://joinup.ec.europa.eu/software/openpermis/home*.
By way of comparison, the current PERMIS code base comprises over 235,000 lines of code, three times the size of Hardened PERMIS. So, using the same estimation methodology, the potential economic value of it to the community is approximately €5M.

Most organisations **customise and build upon** the PERMIS code. Thales [S2] has been working on authorization and Role Based Access Control for a number of years and have said that their "*work would not have been the same without the close cooperation we could establish with Prof. D. W. Chadwick's team at University of Kent*". Recently, Thales has engaged one of its engineering teams to work within a cloud computing collaborative project, under the auspices of OW2, which is an independent, global, open-source software community. The **OpenCloudWare** project covers many aspects of cloud computing, one of these being authorization, which is a subproject led by Thales. The technical directions that they are taking "*are derived from those of PERMIS, which has to be viewed as preliminary, mandatory project, that helped significantly to understand the issues around Attribute Certificates*". Thales is currently delivering a stripped down library for X.509 attribute certificate management that is "*extremely close from the original PERMIS DIS*". Details about this work can be found at http://www.opencloudware.org.

Some organisations have contributed their enhancements back to us, making them freely available to everyone. In particular:
- HP India provided us with source code for using our secure audit service (SAWS) with .NET;
- CCLRC (now the Science and Technology Facilities Council - STFC) [S5] provided us with a Python interface and a .NET interface to PERMIS.

Thales has produced French language variants of various components of PERMIS for use in their French offices, but has not contributed these back to the open source code base as yet.

In summary, PERMIS has had a broad and substantial impact on the security of software used by hundreds of thousands of end users through being incorporated into a range of systems in applications from different sectors including military, commercial, and governmental. The sustainability of the system has been underpinned by the contributions to the open source project from the Swiss Army, HP and STFC amongst others.

5. Sources to corroborate the impact

[S1] **Dr. Eng. Manabu Hirano**, Dept of Information and Computer Engineering, Toyota National College of Technology, has provided a statement
http://www.cs.kent.ac.uk/research/REF2014/Hirano.pdf
[S2] **Pascal Jakobi**, Systems Architect, Thales, 1 av. A. Fresnel, 91767 Palaiseau, France. has provided a statement that validates claims related to Thales.
http://www.cs.kent.ac.uk/research/REF2014/Jakobi.pdf
[S3] **Riccardo Sibilia**, Chief Cyber Threat Analyst of the Swiss Army, Command Support Organisation, Centre for Electronic Operations, commissioned the Swiss software house Ergon to re-engineer PERMIS into Hardened PERMIS, as Kent did not want to undertake this purely programming work. He can validate the claims about Hardened PERMIS.
[S4] **Marcin Szulga**, Head of Research and Development Department, Unizeto Technologies SA is the project manager for the PERMIS project in Poland, and can validate claims related to Unizeto Technologies SA, Poland and the Polish Ministry of Economy.
[S5] **Dr. Neil Geddes** of STFC has given a statement that CCLRC built Python and .NET interfaces for PERMIS. http://www.cs.kent.ac.uk/research/REF2014/Geddes.pdf