Institution: University of Kent		
Unit of Assessment: 11: Computer Science and Informatics		
Title of case study: Advancing the Security, Efficiency, and Innovativeness of Identity Management in Cloud Computing and the Internet through the Implementation of Federated Identity Management		
Period when the underpinning research was undertaken: 2004-2017		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): David Walter Chadwick	**Role(s) (e.g. job title):** Professor of Information Systems Security	**Period employed by submitting HEI:** 2004-2020
Period when the claimed impact occurred: August 2013-2020		
Is this case study continued from a case study submitted in 2014? Yes		

1. Summary of the impact (indicative maximum 100 words)

From 2004 to 2017, University of Kent researchers developed novel federated identity management (FIM) and privilege access management (PAM) technologies, which have been integrated in OpenStack since November 2013. OpenStack is a community cloud project involving 135+ international leading vendors, including Lenovo, Oracle, RedHat, IBM, Rackspace, and Cisco. FIM allows OpenStack users to use their existing usernames and passwords, instead of having to create a new pair whenever they want to access a new cloud service. Introducing FIM has been recognised by OpenStack for accelerating and shaping the project's federated identity system's performance and by OpenStack users for advancing their organisational security and efficiency whilst also saving significant costs.

2. Underpinning research (indicative maximum 500 words)

Background

Since **2004**, Professor Chadwick and his team in the School of Computing at Kent have undertaken extensive research in the field of Information Systems security. The work began with the development of PERMIS – a suite of open-source privilege and access management (PAM) software that provides novel authorisation technologies to developers' software systems. This was the subject of an impact case study in REF2014. Since **2009**, the research has progressed into the novel application area of federated identity management (FIM).

The underlying problem addressed by the research was the hundreds of usernames and passwords that users are forced to remember, which leads to significant vulnerabilities. FIM greatly reduces this number by allowing a single identity provider (using one username/password) to log a user into dozens of federated systems. The FIM research has been of practical benefit to OpenStack – the most popular open source cloud software in the world that has a membership of 135+ international organisations, including global vendors such as Lenovo, Oracle, RedHat, IBM, Rackspace, Cisco, Dell, Fujitsu and Huawei. Prior to November 2013, OpenStack only supported traditional access control methods by individually allocating new usernames and passwords to users – a process that reduced security, impeded business proficiency, and wasted time for both users and service providers. The work on FIM changed that by allowing users to authenticate to an OpenStack cloud using their existing credentials through an external Identity Provider, rather than creating another username and password pair for a particular OpenStack cloud.

The research

Chadwick’s reputation and expertise in the field of system security led to him being invited to present the concept of FIM at FOSAD **2008**. The International School on Foundations of Security Analysis and Design (FOSAD) is one of the foremost events for disseminating knowledge in the area of computer systems and networks security. In **2009**, the presentation evolved into a seminal and highly-cited paper that provides an introduction to digital identity, identity management, and FIM, and the key issues faced, as well as ideas on how to address them **[R1]**.

In **2011**, following the work on PERMIS **[G1]** and the FOSAD talk, Chadwick responded to an ESPRC call for cloud computing with an argument for the integration of FIM. The resulting funded project **[G4]** led to the publication of an introductory paper **[R2]**, which describes a policy-based authorisation infrastructure that can be used by cloud providers to ensure that the users’ privacy policies are stuck to their data. This was followed by a paper demonstrating the feasibility of a policy-based authorisation infrastructure in cloud infrastructure **[R3]**, and a final results paper that describes open source software to support a trust, privacy and security infrastructure for the cloud **[R4]**.

This research initiated Chadwick’s collaboration with OpenStack. He presented the approach at several OpenStack meetings between **2011** and **2013**. Since there were many different FIM protocols in use and still in development, one of the key challenges was how to support *interoperability*. The concept, *protocol independent FIM*, was adopted by the OpenStack developers and now all OpenStack releases support FIM with several protocols supported as standard.

Furthermore, new FIM protocols can easily be added, as and when they are developed. The incorporation of FIM into OpenStack was demonstrated in **2014** in **[R5]**, which presents a detailed federated identity protocol sequence. The paper also describes the implementation of the protocol independent system components, along with the incorporation of two different FIM protocols, namely SAML and Keystone. The FIM protocols were further validated through GÉANT's CLASSe project (**2013-2015**) **[G6]**, which showed how cloud services such as OpenStack can be smoothly integrated in a federation built with an AAA (Authentication, Authorisation, and Accounting) infrastructure, by using Application Bridging for Federated Access Beyond Web (ABFAB) technologies **[R6]**.

3. References to the research (indicative maximum of six references)

[R1] **Chadwick, D.** (**2009**). ‘Federated Identity Management’. In: Aldini, A., Barthe, G. and Gorrieri, R. eds. *FOSAD 2008/2009*. Berlin: Springer-Verlag, pp. 182-196. http://dx.doi.org/10.1007/978-3-642-03829-7_3. https://kar.kent.ac.uk/30609/

[R2] **Chadwick, D**., Lievens, S., den Hartog, J., Pashalidis, A. and Alhadeff, J. (**2011**). ‘My Private Cloud Overview: A Trust, Privacy and Security Infrastructure for the Cloud’. In: *2011 IEEE 4th International Conference on Cloud Computing*, pp. 752-753. http://dx.doi.org/10.1109/CLOUD.2011.113. https://kar.kent.ac.uk/43198/

[R3] **Chadwick, D.** and Fatema, K. (**2012**). ‘A privacy preserving authorisation system for the cloud’. *Journal of Computer and System Sciences*, 78(5):1359-1373. ISSN 0022-0000. https://doi.org/10.1016/j.jcss.2011.12.019. https://kar.kent.ac.uk/31975/

[R4] **Chadwick, D**., Casenove, M. and Siu, K. (**2013**). ‘My private cloud--granting federated access to cloud resources’. *Journal of Cloud Computing*, 2:1-16. http://dx.doi.org/10.1186/2192-113X-2-3. https://kar.kent.ac.uk/43204/

[R5] **Chadwick, D**., Siu, K., Lee, C., Fouillat, Y. and Germonville, D. (**2014**). ‘Adding Federated Identity Management to OpenStack’. *Journal of Grid Computing*, 12:3-27. http://dx.doi.org/10.1007/s10723-013-9283-2. https://kar.kent.ac.uk/43212/

[R6] Pérez Méndez, A., López Millán, G., Marín López, R., **Chadwick, D.** and Schechtman Sette, I. (**2017**). 'Integrating an AAA-based federation mechanism for OpenStack–The CLASSe view'. *Concurrency and Computation: Practice and Experience*, 29 (12). Article Number 4148. ISSN 1532-0626. http://dx.doi.org/10.1002/cpe.4148. https://kar.kent.ac.uk/61206/

Awards and Grants

[G1] SIPS grant (**2004-2006**). 'Seamlessly Integrating PERMIS and Shibboleth'. PI: David Chadwick. Value £61,000.

[G2] DyCom grant (**2004-2007**). **'**Multilayer Privilege Management for Dynamic Collaborative Scientific Communities over Environmental eScience Data Grids'. PI: David Chadwick (Joint bid with CLRCC). Total Value: £185K (£77,000 for Kent).

[G3] DyVOSE grant (**2004-2006**). 'Dynamic Virtual Organisations in e-Science Education'. PI: David Chadwick (Joint bid with National eScience Centre Edinburgh, University of Glasgow, EDINA). Total Value: £283K (£107,500 for Kent).

[G4] EPSRC EP/I034181/1 (**2011**). 'My Private Cloud'. PI: Chadwick. Value £57,808.

[G5] EPSRC EP/J020354/1 (**2012-2013**). 'Sticky Policy Based Open Source Security APIs for the Cloud'. PI: Chadwick. Value: £126,939.

[G6] EC GÉANT grant **(2013-2015**). 'Cloud-ABFAB Federation Services in Eduroam (CLASSe)'. PI: David Chadwick. Value: €89,000.

4. Details of the impact (indicative maximum 750 words)

Advancing OpenStack's commercial innovativeness and efficiency

Chadwick was invited to the OpenStack summits in the USA in 2012 and 2013 to discuss the Kent research on FIM, educating and informing OpenStack stakeholders on its processes through the discussion of key blueprints **[a]**. As a result, in **November 2013** Chadwick's novel FIM design was implemented in the 'H' phase of OpenStack, adding federated access to Keystone (OpenStack's identity manager) **[a][b]**. The Kent FIM protocol was the first (and remains the only) system to have introduced federated identity to OpenStack, and since its implementation in **November 2013** Chadwick has continued to support OpenStack and its developers and users via his advisory role in the Keystone working group (**2011-2017**).

In response to Chadwick's continued contribution and support of the Kent FIM, OpenStack's Keystone Project Lead, Steve Martinelli, stated: 'David [Chadwick] and his team['s …] expertise and guidance in the area of Federated Identity has been priceless. I can confidently say that their collaboration and background on the subject has helped accelerate and shape Keystone's support of Federated identity […] David's opinion is sought out when discussing Keystone issues on OpenStack's mailing list, where his deep understanding of security, and identity management is made evident. The same can be said about David's involvement at OpenStack summits (our bi-annual design conferences), where he is involved in the architectural design of new Keystone features' **[c]**.

Jisc – a company supporting institutions of higher education and research in the UK – also benefits, as stated by Stefan Paetow, Jisc's Research Liaison Coordinator: 'University of Kent readied the Openstack software stack for use with federated identity technologies, including Moonshot, by piloting Openstack with the pre-Assent Moonshot pilot infrastructure and the UK Access Management Federation, submitting fixes to Openstack and Jisc where required, and driving the web-based use case for Moonshot forward' **[d]**.

Improving OpenStack developer proficiency

Many developers are interacting with OpenStack in order to use its interface. Of these developers, Chadwick has advised and educated many as a result of his consultancy via the OpenStack summits and working group mailing list. His Kent team has also generated many new lines of code or patches, for instance, to enhance the usability and proficiency of the software. A senior manager at RackSpace identified that between **2011** and **2014**: 'University of Kent has contributed 1400 lines of code, 102 reviews, 71 patches, 14 blueprints [and…] have been approachable subject matter experts, whose knowledge was widely adopted by the Keystone community' **[e]**. Similarly, an engineer from RedHat in **2017** stated that: 'Professor Chadwick was essential in enabling the project to properly implement Identity Federation, a set of features without which OpenStack would be unusable by a great many organizations […]. As a software engineer at Red Hat, I have seen a direct correlation between the success of our implementation and the work that Professor Chadwick and his team contributed to the project' **[f]**.

Enhancing OpenStack users' security and cost-effectiveness while reducing administrative burden

Users save time and effort while increasing security, because with FIM, users do not have to create and remember a large number of different passwords. Having to create and memorise numerous passwords leads users to choose weak and easily crackable passwords. With FIM, they need to create and maintain only one strong password.

Over 135 international organisations are currently utilising OpenStack, and running their jobs and applications off it. We carried out a survey of OpenStack users to assess the impact of having FIM integrated into Open Stack **[g]**. Sixty per cent of the respondents (n=14) stated that adopting FIM makes the system more (or much more) secure. A Cloud Manager from a national computer network for universities and research noted: '[we] don't have to manage safety of credentials, since we store none. We are not subject to brute-force, since services are accessed via identity tokens only' **[g]**. The Head of Identity Management of the same institution noted further: 'No passwords inserted in web forms, no passwords kept in the keystone, no recovery/force-passwords-on-the-phone, etc.' **[g]**.

Traceability is important as part of implementing security, and this is facilitated by FIM. A System Administrator at a small company highlights the benefit of FIM: 'We will get to know who accesses what and when', while a researcher pointed out: 'R&S and Sirtfi [Security Incident Response Trust Framework for Federated Identity] helps. Also using the institutional accounts helps with traceability' **[g]**. Similarly, an organisation's security relies on a proper audit of their users. For example, it is imperative to revoke access from former employees who had left the organisation. Evidently, the advantage of FIM is clear, as further established by one Network Engineer: 'We can audit access controls from a central system and we can easily require MFA (Multi Factor Authentication) for user logins' **[g]**. This is echoed by an Administrator/Architect from an American telecommunications company dealing with several thousand users: 'Old account remove quicker'; this echoes the view of a Technical Architect at another organisation, who states: 'revocation is central. Centralized group management assignment are key as well' **[g]**.

In addition, FIM offers a potential for saving time and money. The time-saving benefit of having FIM is highlighted by a Cloud Manager from a European institution: 'Registration time is just few clicks wrt [with respect to] alternative procedure for identity verification' **[g]**. An Administrator at a large American telecommunications company elaborated further: 'Multiple Operation people were spending >30% of their time just managing accounts before we implemented hooking into corporate Active Directory System' [g]. Meanwhile, a Cloud Architect at a UK Government agency believed that FIM reduces operational costs, affording a saving of '0.5 of a person to maintain the identity proxy' **[g]**. Similarly, a System Administrator at a small company noted a saving of 'roughly $5000', while the Head of Identity Management at a European institution reported a saving of '0.2 FTE' **[g]**.

Administrative burden can also be reduced by using FIM, with 47% (n=11) of the respondents suggesting that there is less or much less administrative burden in running their system. A Senior Software Engineer at a public open cloud exchange project commented: 'A unified authentication management has allowed us to let users use the same accounts for OpenStack and OpenShift, which we are operating. So we and users don't have to deal with multiple accounts or systems of access management […] Also we can offload verifying a user to the identity providers they are coming from' **[g]**. A Technical Specialist at a European organisation pointed out: 'when a user leaves the home organisation, and his account is deactivated, this user cannot log in anymore in the open stack environment. Effectively, his permissions are revoked while openstack maintainers don't know (and now don't care) that he is gone' **[g]**. A Cloud Platform Architect at a multinational telecommunications company summarised the impact in reference to his 3,600 users: 'No more account management, users shall do it for us' **[g]**.

Based on his FIM research and as a result of the growing recognition of his expertise in this field, Chadwick was an invited expert to the nascent W3C Verifiable Credentials working group in **2017**. His contribution led to his co-authorship of the Recommendation and its associated Implementation Guidelines **[h]** and Data Model **[i]**. In **2019**, the University created a spin-out company, Verifiable Credentials Ltd, to capitalise on the implemented Proof of Concept.

5. Sources to corroborate the impact (indicative maximum of 10 references)

[a] Keystone/Federation/Blueprint Web-clipping: Presents the final version of the blueprint developed following the OpenStack Summit and describes how to add protocol independent federated access to Keystone, the identity service of OpenStack. https://wiki.openstack.org/wiki/Keystone/Federation/Blueprint

[b] Presentation by CERN at the OpenStack summit in Hong Kong in Nov 2013. Slide 24 reveals the pathway to impact that Kent has had on CERN's efforts by collaborating with them. https://www.slideshare.net/andrewrhickey/cern-rackspaceopen-stacksummit

[c] Letter from OpenStack's Keystone Project Lead at IBM, describing Chadwick's continued contribution to help accelerate and shape Keystone's support of Federated Identity (26 November 2015).

[d] Letter from Moonshot Industry & Research Liaison Coordinator at Jisc, describing the University of Kent's contribution in vital resources and research to the development and testing of the Moonshot technology (14 January 2016).

[e] Letter from the Senior Manager, Product at Rackspace, describing the contributions of Chadwick's team to improving OpenStack developers' proficiency (30 November 2015).

[f] Letter from Cloud Solutions Architect at Red Hat, Inc., describing the essential role played by Chadwick in enabling OpenStack to properly implement Federated Identity (15 November 2017).

[g] Survey data of OpenStack Stakeholders, based on input from 23 stakeholders, including service providers and service users (23 December 2019 to 31 January 2020).

[h] W3C Verifiable Credentials Implementation Guidelines 1.0: Implementation guidance for Verifiable Credentials (24 September 2019). https://www.w3.org/TR/vc-imp-guide/

[i] W3C Verifiable Credentials Data Model 1.0: Expressing verifiable information on the Web (19 November 2019). https://www.w3.org/TR/vc-data-model/