Institution: University College London

Unit of Assessment: 11 – Computer Science and Informatics

Title of case study: Human-centred security in government and commercial applications

1. Summary of the impact

Professor Sasse created, developed and delivered the user-centric perspective that now underpins security thinking in both corporate and public-sector domains. This perspective shaped the UK government's Identity Assurance Programme (IDAP), a federated identity solution that will provide access to all e-government services in the UK. HP has incorporated the compliance budget model into its Security Analytics product, which enables companies to calculate the impact of a given security mechanism on individual and corporate productivity. Sasse's work also underpins new and improved security products, including First Cyber Security's SOLID and Safe Shop Window tools, which protects over 70% of UK online shopping revenue; GrIDSure's one-time PIN system (now part of the SafeNet Authentication Service); and iProov's authentication service.

2. Underpinning research

The human-centred approach – which prioritises the design of usable security that works with and for, rather than against, users and their organisations – was first formulated by Professor Sasse (Professor of Human-Centred Technology; at UCL since 1990) in 1999 in her groundbreaking CACM paper: "Users are not the enemy"; it has been cited over 800 times and is recognised as one of the founding papers of Usable Security [1]. It unpicked how security policies and mechanisms that are too difficult to use lead to productivity losses, non-compliance and errors, and a negative security culture. Security policies and mechanisms implemented without considering the users thus consume considerable organisational resources, but do not deliver effective security. When BT hired Sasse to conduct the study, forgotten passwords consumed huge help desk resources, at ever-increasing cost to the company. The paper led to the introduction of single sign-on solutions, less complex password content, and longer password expiry periods.

In 2008, she developed the **compliance budget concept**, which explains how friction between information security and business process reduces both security compliance and personal and organisational productivity [2]. An analysis of users' security burden in economic terms showed that security measures need to be seen in context with all the other demands on a user's time and attention. The user's ability to comply – the "compliance budget" – is limited and needs to be managed like any other finite corporate resource. Collaborating with HP Labs in Bristol from 2008 to 2012, she integrated user behaviour into economics and system modelling research in order to integrate the Compliance Budget into a large-scale organisational model allowing predictions of the cost and effectiveness of security policies and mechanisms [3]. Rather than focusing on theoretical risk mitigation that can be achieved through the introduction of security mechanisms, UCL's research suggested policies should be designed using human-computer interaction (HCI) principles to make it easier for users to 'do the right thing' when it comes to security.

In most organisations, IT security managers decided on security policies and mechanisms without considering the impact on individual and corporate productivity. The work presented a new approach that incorporates the impact of security controls on users' productivity and willingness to comply into business impact and risk reduction [4]. As part of this, Professor Sasse pioneered the use of quantitative and qualitative data collection and analysis methods (system logs, user diaries and surveys based on security dilemmas) to obtain evidence of the impact and effectiveness of security measures [5].

These methods were used in a project commissioned by the US National Institute of Standards and Technology (NIST) to collect evidence for the productivity losses caused by the 'wall of disruption' created by outdated explicit authentication mechanisms, and to make the economic case for the introduction of implicit authentication mechanisms – for which Sasse coined the term "0 effort, 1 step, 2 factor" authentication. She also pioneered the use of web-based authentication field trials to monitor the long-term authentication performance of novel mechanisms, and ways of

influencing users to pick 'less obvious', yet memorable choices [6].

In 2012 she extended the compliance budget concept into the more ambitious concept of **productive security:** security measures not only reduce specific risks, but provide additional value to other aspects of the business process, such as quality enhancement, more fine-grained customer feedback and personalisation. Productive security is a structured decision-making framework into which company data can be inserted, alongside the key 'missing link' measurements of employee's workload, risk perception, and resulting security behaviours. This helps companies understand the total cost of ownership of security measures, thereby choosing security mechanisms that improve other aspects of the business process leading to an overall increase of productivity of the organisation. Mechanisms that involve, rather than antagonise, individuals are an essential part of a more flexible capability to defend against as yet unknown security threats, against which engaged and watchful staff provide the 'last line of defence'. The research to demonstrate the impact of this idea is funded by GCHQ and EPSRC as part of the Research Institute in Science of Cyber Security (of which Sasse is Director) and conducted *in situ* with three major UK companies and one public sector organisation (identities not revealed for contractual reasons).

Researchers working in Professor Sasse's team were: Adam Beautement (RA since 2012), Sacha Brostoff (RA at UCL 2006-2007 and 2009-2012), Philip Inglesant (RA at UCL 2008-2011), and Simon Parkin (involved 2008-2012 while working at Newcastle and HP, joined UCL as Senior RA 2012).

3. References to the research

References 1, 2 and 5 best demonstrate the quality of the research.

1. Adams, A., Sasse, M. A. (1999). Users are not the enemy. COMMUN ACM 42(12), 41-46 http://doi.org/dk64zz

2. Beautement, A., Sasse, M. A., Wonham, M. (2008). The Compliance Budget: Managing Security Behaviour in Organisations. *Proceedings of the 2008 workshop on New security paradigms*. (pp.47-58). Lake Tahoe, California, USA: ACM. http://doi.org/dt3w54

3. Beautement, A., Coles, R., Griffin, J., Ioannidis, C., Monahan, B., Pym, D., Sasse, A., Wonham, M. (2009). Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security, in *Managing Information Risk and the Economics of Security*. (pp.141-163). Springer US. http://doi.org/ckhn5v

4. Parkin, S., van Moorsel, A., Inglesant, P., Sasse, M. A. (2010). A stealth approach to usable security: Helping IT security managers to identify workable security solutions. *NSPW '10: Proceedings of the 2010 Workshop on New Security Paradigms.* (pp.33-49). New York, US: ACM Press http://doi.org/dd6t58

5. Inglesant, P., Sasse, M. A. (2010). The True Cost of Unusable Password Policies: Password Use in the Wild. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 10)*. (pp.383-392). ACM. http://doi.org/bd548c

6. Jhawar, R., Inglesant, P. G., Sasse, M. A., Courtois, N. T. (2011). Make mine a quadruple: Strengthening the security of graphical one-time PIN authentication. *Proceedings of 5th International Conference on Network and System Security (NSS 2011).* (pp.81-88). http://doi.org/c6hpcc

The research outlined above has been supported by **major grant funding** of almost £2 million from NIST, GCHQ, the EU, EPSRC and TSB. The Productive Security work has received £870K of EPSRC funding as part of the Research Institute in Science of Cyber Security (total £3.8M), of which Sasse is Director. Sasse received an additional £300K for the Research Institute coordination activity.

4. Details of the impact

The concepts developed by Professor Sasse through the research described above have transformed the delivery of effective security by UK government and industry. By informing improvements in the design of security systems used by millions of people each day, Sasse's work has helped make systems easier to use while reducing the risk of security breaches in service provision. Her work has also led to widespread commercial benefits, with the production of improved security products and greater organisational efficiency stemming from more usable and cost-effective systems. As of 2013, the human-centred approach to security is now seen by government and industry as standard and essential, and forms the cornerstone of security practices in many large and small corporations globally.

Adoption of new technology in public services: Technology allows for virtually all government services to be made available online in a secure and effective way with simple, user-friendly ways for citizens to assert their identity. This access needs to be consistent across government services whilst being highly secure and able to preserve users' privacy. Between 2008 and 2011, Professor Sasse advised the government on e-government security. Specifically, she was heavily involved in defining and implementing the federated identity solution developed by the Cabinet Office Identity Assurance Programme to ensure a low-cost, low-effort and privacy-respecting way for authenticating UK citizens. In June 2013 the government confirmed this would be the "default service for all government departments providing public digital services which require identity assurance" [a]. This will enable the government to provide online more of its services, for example universal credit, accessing benefits and pensions, passport and driving licence renewal and many more. The system started alpha trials in May 2013, with eight federated identity service providers including the Post Office, Experian and PayPal, involving thousands of service users; a statement from the Cabinet Office confirms its plans that this form of authentication will be used by the majority of the UK's 45 million adult population [b].

New online security products: Between 2008 and 2011 Sasse also worked with several SMEs to deliver usable authentication products such as GridSure and PINplus [c]. Most notably, her work with First Cyber Security led to a redesign of their anti-phishing tool SOLID. One of the biggest difficulties with anti-phishing software is users' failure to notice indicators from the software while on web pages. Sasse's work enabled the company to identify which software design elements to adapt to increase users' intuitiveness and perceived speed, alongside a review of the human interaction with the software [d]. The improvements have led to a huge expansion of the customer base for the tool, which is now used by over 1,000 online retail sites. Sasse's guidance on minimising user effort and giving them value inspired the company to create a new integrated product: the Safe Shop Window, which provides shopping search results that filter out suspicious sites, saving users time as they no longer need to evaluate each site individually. This launched in 2012 and now protects the customers of sites that generate 70% of the UK online retail turnover [e, f].

Sasse is currently Chief Scientific Advisor of iProov, a security startup company that delivers her concept of "0 Effort, 1 Step, 2 Factor" authentication, described above. The company provides an off-the-shelf biometric authentication service for companies, so they do not have to invest in costly and inefficient in-house services. Sasse's work improved the biometric by improving the usability of feedback given to users. Launched in 2011, iProov now employs four full time staff and has recently won two TSB grants, for which the CEO confirms Sasse's engagement made a "material difference". iProov is already bidding for major commercial contracts in the financial, telecommunications and call centre industries. [g]

Adoption of new processes in businesses: During the Trust Economics project (2008-2011, funded with £1 million by UK TSB) Sasse collaborated with HP Labs to include models of human behaviour in security models and tools [h]. Building on this work, since 2011 HP has exported Sasse's user-centred approach in their consultancy to other companies through its Security Analytics service [i]. This calculates the cost to a business of using particular security approaches. It draws on Sasse's expertise in calculating how much employee time is spent dealing with a given mechanism. This enables HP, and by extension its clients, to work out the costs of this silent waste

of productivity, thereby informing the decisions an organisation makes about security. For example, in 2011 one of HP's clients was the University of Nottingham, which was able to identify which areas of its security system did and did not require further investment [j].

5. Sources to corroborate the impact

[a] GDS confirms Identity Assurance as 'the default service' for all departments: http://www.governmentcomputing.com/blogs/gds-confirms-identity-assurance-as-the-default-service-for-all-departments

[b] Letter from the IDAP lead for the Government Digital Service, the Cabinet Office, confirms UCL's contribution to the IDAP programme, and that it affects most of the UK's adult population. Available on request.

[c] A supporting statement from the inventor of GrIDsure and PINplus confirms Sasse's work on the usability of the two companies' products. Available on request.

[d] Corroboration of the improvements to SOLID stemming from Sasse's research project: http://www.firstcybersecurity.com/main/SOLID%20Case%20Study%20Aug%202010.pdf

[e] Statement from the Managing Director of First Cyber Security (FCS), confirms the improvements UCL's research made to the SOLID tool, the number of sites using FCS's technology and Safe Shop Window's validation of 70% (by revenue) of UK shopping sites. Available on request.

[f] First Cyber Security's Safe Shop Window: http://www.safeshopwindow.co.uk/

[g] A statement from the iProov CEO corroborating details about the company (e.g. staff numbers, funding raised, types of client), and the contribution of Professor Sasse's work to the company's success is available on request.

[h] The outcomes of the work with HP Labs is: Trust Economics: A systematic approach to information security decision-making, HP, 2011, http://www.hpl.hp.com/news/2011/oct-dec/Final_Report_collated.pdf

[i] Statement from HP's Technical Solution Director (Innovation & Cloud Security), available on request. This corroborates that UCL's work has benefited HP and its Security Analytics clients. http://www.hpl.hp.com/news/2011/oct-dec/security_analytics.html

[j] "The University of Nottingham benefits from enhanced risk and threat management with advanced information security expertise from HP", http://h20195.www2.hp.com/v2/GetPDF.aspx%2F4AA3-9859EEW.pdf