THE QUARTERLY MAGAZINE OF BCS INTERACTION GROUP

interfaces

www.bcs-hci.org.uk

86 SPRING 2011

USABLE SECURITY

Decades of confusion and no closer to solving the conundrum

bcs The Chartered Institute for IT

Mike Just is a lecturer at Glasgow Caledonian University where his interests include security and human–computer interaction. He spent six years with the Canadian government working to improve the security and usability of their services to citizens and employees. Mike is currently investigating how social interaction with others can assist users and improve the security and usability of the applications they use.

www.gcu.ac.uk/sec/mjust

Karen Renaud is an academic at the University of Glasgow. She has been working in the area of Usable Security for the last decade. Her main focus in the last few years has been to understand the chasm between security professionals and ordinary employees and to find ways of closing the gap.

www.dcs.gla.ac.uk/~karen

Lorrie Faith Cranor is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University, where she is director of the CyLab Usable Privacy and Security Laboratory (CUPS). She is also Chief Scientist of Wombat Security Technologies, Inc. She has authored over 100 research papers on online privacy, usable security, phishing, spam, electronic voting, anonymous publishing, and other topics. She co-edited the seminal book *Security and Usability* and founded the Symposium On Usable Privacy and Security (SOUPS).

lorrie.cranor.org

Alan Dix is a researcher at Talis, a semantic web company based in Birmingham, and Professor of Computing at Lancaster University. He has written widely on human–computer interaction and related areas. He is co-author of *Human–Computer Interaction* and is currently completing *TouchIT*, a book on physicality and design. His interests range from formal methods to creativity, and a colleague and he are the co-inventors of intelligent lighting that is about to go into commercial production.

www.alandix.com

CONTRIBUTORS

With thanks to:
My PhD: Shaun Lawson

BCS membership
To receive your own copy of *Interfaces*, join the BCS and gain access to BCS Interaction and four other Specialist Groups (see page 27).

PDFs of *Interfaces* issues 35–85 can be found on the Interaction website **www.bcs.org/server.php?show=conWebDoc.36812**

About INTERFACES
Interfaces welcomes submissions on any HCI-related topic, including articles, opinion pieces, book reviews and conference reports.

Forthcoming themes
Interfaces 87, Summer 2011: deadline: **30 April 2011**. Theme: Different Perspectives.

Submission guidelines
Articles should be MS Word or plain text. Send images as separate files: these must be high resolution digital originals suitable for commercial printing, cropped if desired but not resized, and if edited, saved as tiff or highest quality jpeg. Please supply photographers' credits as appropriate. Authors should please provide a 70-word biography and a high resolution head and shoulders original digital photo.

Photographers' credits will be printed if provided.

Send to Lynne Coventry, E lynne.coventry@northumbria.ac.uk, T 0191 243 7772
PaCT Lab, Northumberland Building, University of Northumbria,
Newcastle upon Tyne, NE1 8ST

Interfaces is published quarterly by BCS Interaction (a Specialist Group of the BCS) and is available in print and as download. *Interfaces* is produced on a not-for-profit basis by volunteers for the good of the international HCI community. *Interfaces* editorial policy is focused on promoting HCI and its community in all facets, representing its diversity and exemplifying its professional values by promoting knowledge, understanding and awareness to the benefit of all and harm to none. Editorial decisions are based on promoting these core values with the Editor being accountable to BCS Interaction Specialist Group and BCS for the content of the magazine. As such the Editor has the right to refuse publication with recourse to BCS Interaction Specialist Group and BCS in cases of arbitration. The views and opinions expressed in *Interfaces* are strictly those of the relevant authors attributed to articles and do not necessarily represent those of BCS Interaction Specialist Group, BCS or any associated organisation. *Interfaces* does not accept responsibility for the views expressed by contributors and unless explicitly stated (where authors are publishing at the behest of an organisation or group), authors are acting in a personal capacity and expressing personal opinions that may or may not represent the views and opinions of any organisation, employer, person or group attributable to them.

Two decades of counting and confusion best illustrate our understanding of usable security, according to Cormac Herley of Microsoft Research at Financial Cryptography 2011. Counting the exponential rise in the number of internet users and password accounts, yet still confused about the exact nature of the usable security problem.

Alan Dix reports in this issue about recent leaks in personal information, and other large scale leaks have been reported in the press, but what are the consequences of these leaks? Linda Little reports on people's willingness to share different categories of information. In 2009 RockYou suffered a data breach which leaked 32 million passwords. Was this because there was a weak password policy or because passwords were being stored in the clear – so are the users to blame for this?

In 2010 RockYou leaked a top 20 password cloud. Our contributors such as Karen Renaud and M. Angela Sasse point out the continued re-use of passwords, so these credentials could well be used for other applications. Add to this the fact that users also share and give away passwords and we are left with the question of why there has not been the same exponential rise in fraud – is it a well-kept secret or are the security mechanisms that prevent fraudsters cashing in on this knowledge doing their job? Lets hope it's the latter.

Lynne Coventry

CONTENTS

VIEW FROM THE CHAIR

UX AS A TEAM SPORT

Tom McEwan reflects on the scarcity of HCI and UX education, and questions the role of UX understandings in moving innovation beyond trendy repackaging.

One of the more remarkable outcomes from UXCF2010, the first workshop on UX Competency Frameworks, was to see all the participants grow, in the course of the day, to recognise that UX is not delivered by individuals but by teams and organisations. Some already knew this, of course, and various capability maturity models have floated around HCI for over a decade, but for others it was a shock – used, perhaps, to being the lone voice of the user in an otherwise engineering or marketing led organisation or project.

Not perceived as trendy

By the end of the day, we were satisfied that UX teams had a fairly consistent combination of skills and backgrounds, and that enhancing organisational processes helped make these teams effective. Nothing revolutionary there, but again a challenge to educators to identify the curricula that lay the foundations for this. Until now HCI has been paddling furiously beneath the surface to keep its place in the SWEBOKs and model computing curricula. Specialist HCI courses remain thin on the ground, UX even more so, and, when pioneers do get them introduced, they tend to be a minority interest compared to other novel ICT courses, such as security and forensics or digital media.

Yet for all this, ICT companies repeatedly wish that computing graduates had more solid business grounding, appreciation of the market and the customer. When you dig a little deeper it doesn't sound a million miles from UX though they either don't know or dislike the term, just as HCI remains a bit of a TLA.

UX is about more than repackaging

UXCF2011, part of HCI2011, will try to address this mismatch of stakeholders' needs in defining a UX curriculum, but another need is becoming apparent, based on my skimming the dozens of recent postings on our freshened-up **usabilitynews.com**. Much play is made of how successful 'innovative' companies, like Apple and Ikea (to quote one source), don't get where they are today by listening to the user, but rather by letting people have free rein to come up with great products. But, as Karen Holtzblatt observed at INTERACT99, 'skunk works, doesn't'. This kind of 'innovation' certainly produces fashionable repackaging of mature technologies that only need to hang together long enough until fashion requires their replacement.

It's not about 'me, me, me' any more

For me, and I hope for you, UX is more than providing gratification 'because they're worth it'. UX is not just a team sport in its provision, but also in its outcomes. Sociopaths aside, all users have social factors that affect how positive their experience is. While there is a long history of selling based upon 'guilty pleasures', few of us really enjoy something if we are aware of socially irresponsible manufacture. So we have turned to brands such as Fairtrade to give us some reassurance. A degree of transparency in the production process salves our consciences and makes actually pretty tasteless chocolate somehow more enjoyable. One source of guilt somehow more pleasurable than two guilts plus enhanced gratification?

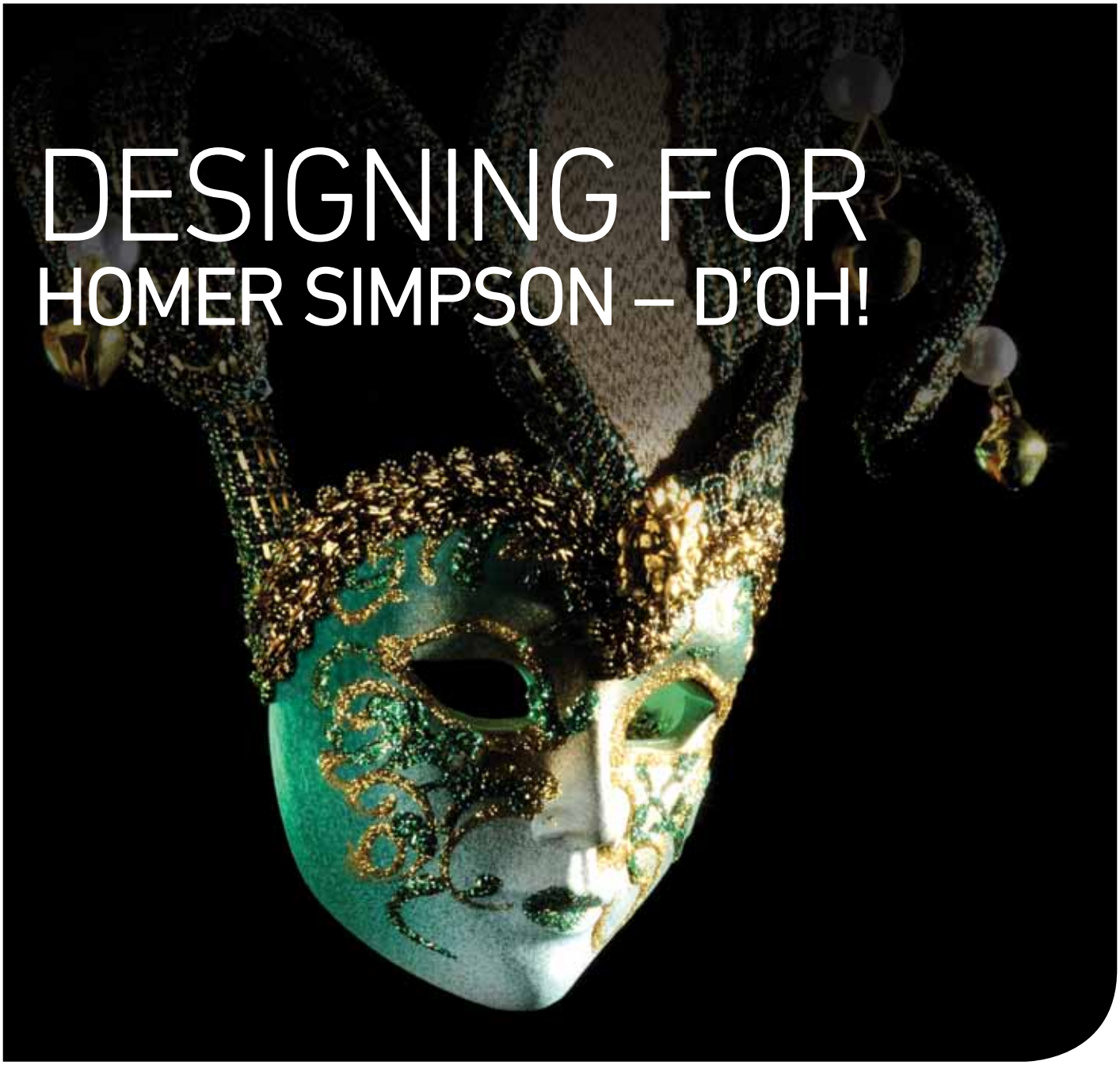
The HCI community is a very enjoyable place to be because you meet so many likeable people, all of whom fundamentally seem to have other people's interests at heart. What HCI can offer UX is something more fit for purpose than 'me generation' manipulations. It can broaden the scope of UX beyond affect, aesthetics and ease of use, to embracing social responsibility, civic society and a sustainable environment.

I'll close by noting that Joanna Bawa stepped down at the end of the year as the long-serving editor of UsabilityNews. On behalf of the committee, the membership and the viewers, thank you for all your hard work, Jo, we'll all miss your enthusiasm and eye for a story, and we hope you'll keep in touch.

Tom McEwan
BCS Interaction SG Chair
Edinburgh Napier University

T.McEwan@napier.ac.uk

DESIGNING FOR HOMER SIMPSON – D'OH!



Professor M. Angela Sasse (UCL), while acknowledging that the field of usable security has flourished over the last decade, feels that too many people miss the point and follow the 'design for dummies' philosophy rather than truly understanding human-centred security.

Modern security researchers have generally acknowledged that – to achieve effective security – they must consider how the mechanisms they design affect the humans that have to use them. In their seminal paper setting out principles of information security, Saltzer and Schroeder (1995) identified *psychological acceptability* of security mechanisms as a necessary condition for their success. Zurko and Simon (1996) were the first to point out that computer security was beginning to place increasing – and increasingly unacceptable – demands on users, system administrators, and software developers.

Two case studies published a little over a decade ago started the research area known as usable security (or HCISec) today: In 'Why Johnny can't encrypt', Whitten and Tygar (1999) reported results from a user trial of the email encryption tool PGP – to be precise, of version 5, the first to have a graphical user interface (GUI). They found that despite the GUI, most participants did not manage to send their email encrypted. Arguably even more worrying was that most of the participants who failed to encrypt their email thought they had.

Whitten and Tygar identified a range of causes for these problems, the main one being the failure to represent users' task models and language in the interface, and lack of feedback of user actions. In 'Users are not the Enemy', Adams and Sasse (1999) reported findings from a study of password problems in a commercial organisation. They found that employees were unable to cope with the workload generated by the number and complexity of passwords required by the organisation's security policies. Employees created a number of workarounds – such as writing passwords down in plain sight – to cope with the unmanageable workload. Arguably of even greater concern was that these problems affected employees' perceptions of, and attitudes to, security – they thought the main purpose of security was to place obstacles in the path of completing the main production tasks, on which they are assessed.

Is it time for congratulations?
Since those early days, research in usable security has flourished: there are several substantial research groups in the US and the UK, we have our own conference, the ACM Symposium on Usable Security and Privacy (SOUPS, founded by Lorrie Cranor at CMU), and mainstream security and usability conferences (such as ACM CHI and BCS HCI) have accepted the output of this research. There are university courses, and a few books. So – can we congratulate ourselves on a job well done?

Security is even more of a burden for users now
We cannot, because for individual consumers, and employees in commercial organisations, little has changed. Johnny still can't encrypt: while encryption and signing of email could offer valuable protection against many current security threats – such as phishing – these mechanisms have not been widely adopted. A decade ago, thought leaders in usability (Jacob Nielsen) and security (Bruce Schneier, Bill Gates) confidently predicted that passwords would not trouble users any longer because they were about to be replaced (for instance by biometrics, assumed to be 'inherently usable').

We recently studied the impact of passwords on employees in two organisations and found that, despite the introduction of Single Sign-On mechanisms, employees still had more passwords than they could cope with, and experienced significant disruption of their work (Inglesant and Sasse, 2010). We still observed coping strategies around passwords – though they were generally more discreet than writing passwords down in plain sight.

For most individuals, the workload and complexity of authentication has increased: at the time of the 'Enemy' study, employees with authentication problems only had to deal with passwords and helpdesks. Today, individuals – in their roles as employees or customers – have to also register and recall back-up questions, carry out self-service re-sets, and decipher increasingly difficult CAPTCHAs (those unreadable letters you have to figure out and type in, to prove you are human).

Employers and service providers clearly still think that the cost of dealing with (1) the failure of authentication that is too difficult in the first place, and (2) threats that they face (such as attackers trying to create accounts for botnets and spam) can be dumped on individual users. They consider it reasonable to ask people to study security indicators before going to any website, and refrain from interacting with any website that triggers a certificate warning. They blame individuals for not being sufficiently aware of security threats, or being too lazy to keep their machines patched and their virus-checkers and firewalls up to date. Cormac Herley (2009) brilliantly summarises that security practitioners essentially '... treat the user's attention and effort as an unlimited resource'.

Why is usable security not having an impact?
So why has usable security research failed to make an impact on this sorry state of affairs? Are those in charge of security still ignorant about the impact that their security measures have on users? In my experience, most security folk understand that placing too many demands on users' time and attention is counter-productive, and that only usable security is effective security. The problem is that they have a shallow understanding of what usable security means in practice. Over the past year, I have heard two eminent security researchers – one each from academia and industry – say that usable security means 'designing security for Homer Simpson', i.e. designing for people who are stupid, lazy, and willing to put everything at risk for a doughnut. It is an unwelcome re-phrasing of an earlier security catchphrase: 'people are the weakest link'. This is an unhelpful myth we tried to dispel a decade ago, but security has still not grasped the basic principles of human-centred design we were trying to promote (Sasse et al., 2001).

We need to look at security from a different perspective
This means we have to keep reiterating to the security community what human-centred security means. Human-centred security is designed to fit human capabilities and limitations, and does not generate unreasonable demands and workloads. It also needs to fit with the values that users have – security designers should ask what users want to protect (Friedman et al., 2002), and offer simple, reliable information regarding choices they should be free to make, rather than scare users into compliance by spreading fear, uncertainty, and doubt (FUD). Security needs to have a notion of users' goals, and the activities they carry out to achieve them; it needs to fit into those activities, rather than

create conflicting goals and disrupt users' primary activities (Whitten and Tygar, 1999). Finally, it needs to fit with the physical and social context in which the interaction takes place. Some companies already understand these principles and design security accordingly. Amazon.com, for instance, realised that some customers need a facility for 'electronic pocket money' – allowances an account holder can give to family members to spend online. The Amazon *payphrase* allows customers to give such allowances, without sharing credit card information, and to set controls on what the money can be spent on. A welcome recent research strand – security by design – aims to encapsulate these principles into software engineering models (Failey and Fléchais, 2010) and uses approaches from human-centred design, such as personas and scenarios, to represent the needs, values and activities of all key actors.

Understanding the cost of security for its users

The second strand of research combines and aligns usability and the economics of security. Cormac Herley in the US (Herley, 2009) and the Trust Economics project in the UK (Beautement, 2008) have started to quantify the impact of security mechanisms on individual productivity. The latter research activity has produced tools that factor the impact on users into the cost of operating security in an organisation (Beautement, 2008). There is now a growing realisation that the time and effort that users will expend on security is limited; individuals instinctively realise when the demands associated with security are counter-productive and unsustainable in the long run. When too much user effort is diverted from their primary, productive, activity, they will try to circumvent security mechanisms rather than comply with security policies. Interviews with employees on compliance with security policies found that this limit applies to individual security tasks, and to cumulative effort over time. This led to the formulation of the Compliance Budget, which re-conceptualises user effort as a limited resource that has to be spent wisely if the organisation wants users to comply with important security measures. For corporate decision-makers – generally Chief Information Security Officers (CISOs) – the Trust Economics project has developed a dashboard-style interface that shows the impact of security mechanisms on different groups of employees in the organisation (Parkin et al, 2010). Our research with CISOs showed that they did not know how to apply research findings on the usability and economic impact of security measures when making a decision about a specific security policy or measure. This led us to consider CISOs as a user; rather than trying to educate them about usable security, we took the stealth approach of packaging and presenting knowledge of the impacts that security has upon users within a tool that CISOs can draw on during the security management decision-making process, to make more informed choices about the security mechanisms they deploy within their organisations.

It's time to achieve the age-old principles

These recent research activities will, we hope, lead to significant changes in how security is designed, and how decision-makers think about it. Interestingly, it turns out that this 'new security thinking' has a noble tradition. The founding father of cryptography, Auguste Kerckhoffs, set out six principles for effective secure communication in 1883. Amazingly, three of the six are concerned with usability:

> Principle 3: It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
>
> Principle 5: The system must be portable, and its use must not require more than one person;
>
> Principle 6: Finally, regarding the circumstances in which such system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Usable security research is helping the security community to re-discover the foundations on which effective operational security is based: a human-centred perspective designs security to match the strengths, limitations and values of humans, the goals of individual and collective activity, and the context which this activity takes place. I like to think that Kerckhoffs is very glad that usability researchers took an interest in the discipline he founded. But we still have work to do.

Acknowledgements

Many thanks to Ivan Fléchais (Computer Lab, Oxford University) for pointing out Kerckhoffs' principles, and for inspiring the title of this article in one of our many discussions on this topic.

REFERENCES

Adams, A. and Sasse, M.A. (1999). Users are not the Enemy. *Communications of the ACM*, **42**:12, 40–46.

Beautement, A., Coles, R., Griffin, J., Monahan, B., Pym, D., Sasse, M.A., and Wonham, M. (2008). Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security. In *Procs Workshop on Economics in Information Security* (WEIS).

Beautement, A., Sasse, M.A. and Wonham, M. (2008). The Compliance Budget: Managing Security Behaviour in Organisations. In *Procs of the New Security Paradigms Workshop.*

Faily, S.and Fléchais, I. (2010). Analysing and Visualising Security and Usability in IRIS. In *Procs Fifth International Conference on Availability, Reliability and Security*, (ARES 2010).

Friedman, B., Howe, D.C. and Felten, E. (2002). Informed Consent in the Mozilla Browser: Implementing Value Sensitive Design. In *Procs of the 35th Annual Hawaii International Conference on System Sciences* (HICSS'02), **8**.

Herley, C. (2009). So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Procs 2009 Workshop on New Security Paradigms.*

Inglesant, P.G. and Sasse, M.A. (2010). The true cost of unusable password policies: password use in the wild. In *Procs of 28th international conference on Human factors in computing systems* (CHI '10), 383–392.

Kerckhoffs, A. (1883). La cryptographie militaire, *Journal des Sciences Militaires*, 5–38.

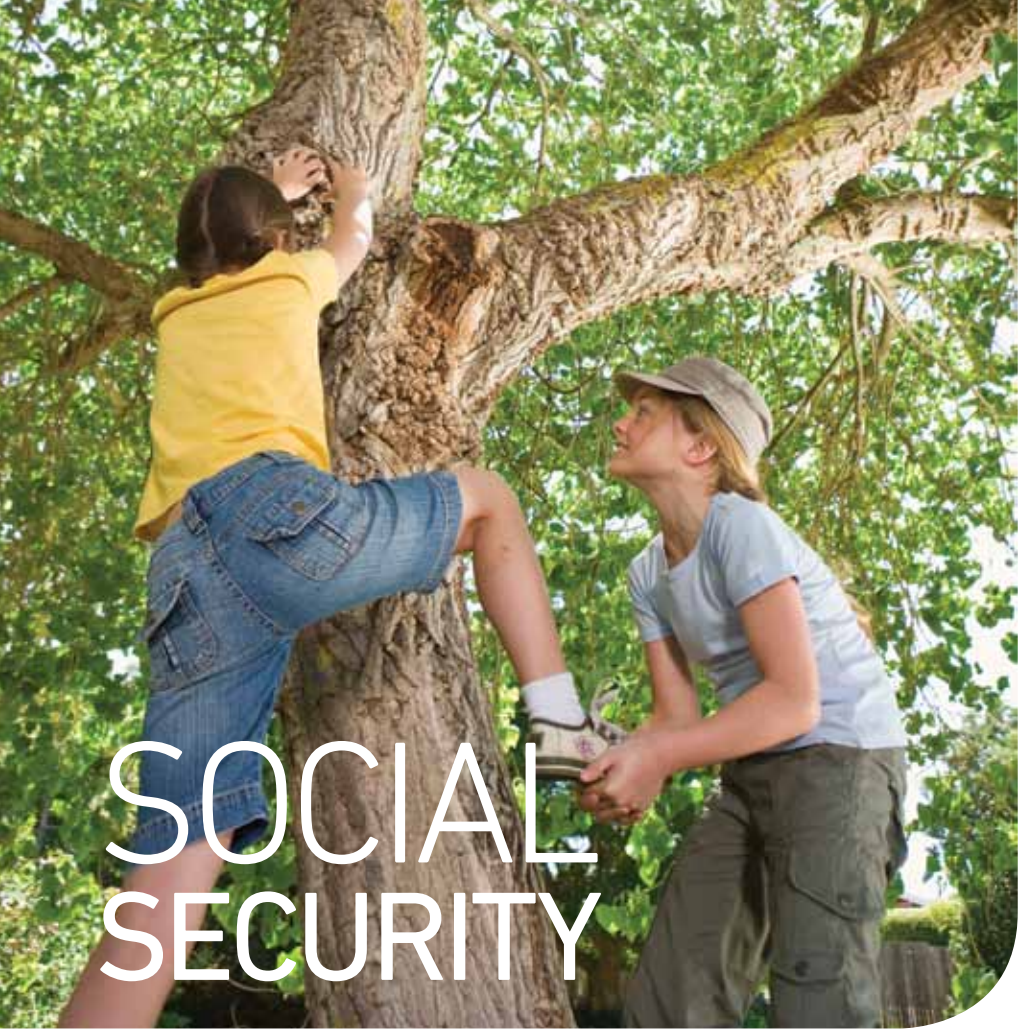
Parkin, S., Van Morsel, A., Inglesant, P. and Sasse, M.A. (2010). A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions. In *Procs of the New Security Paradigms Workshop.*

Saltzer, J. and Schroeder, M. (1975). The protection of information in computer systems. In *Proceedings of the IEEE* **63**:9 (September 1975), 1278–1308.

Sasse, M.A., Brostoff, S. and Weirich, D. (2001). Transforming the 'Weakest Link': a human–computer interaction approach to usable and effective security. *BT Technology Journal 2001*, **19,** 122–131.

Whitten, A. and Tygar, J.D. (1999). Why Johnny Can't Encrypt: a Usability Evaluation of PGP 5.0. In *Procs of the 8th Conference on USENIX Security Symposium.*

Zurko, M.E. and Simon, R.T. (1996). User-centered security. In *Procs of the. New Security Paradigms Workshop*, CA, USA, 27–33. ACM.



SOCIAL SECURITY

Mike Just of the University of Edinburgh pursues usable security with a little help from his friends.

I am a computer scientist and I struggle with technology. The claimed convenient experience of online interaction feels far from enjoyable when I undertake tasks such as online purchases or moderately complex searches for information. Security applications are by no means exempt from this reality. Usable security has been recognised as a challenge for many years (Adams and Sasse, 1999) and is the subject of numerous research efforts (Cranor and Garfinkel, 2005). Certainly there some well-designed applications, but I am often left frustrated and disappointed from my technology interactions.

At the same time, today's world bears witness to a significant increase in online social interaction. Examples abound, and include file sharing for music and movies, crowdsourcing for problem solving, and mashups for combining disparate data into a single application. The applications are surprisingly broad, helping users to perform certain tasks better, but also allowing them do things that they might not otherwise be able to do. In some cases the social interaction is obvious and explicit, while in other situations it might be implicit, where previous experiences and results feed into another user's decisions.

Social assistance

At first blush, social interaction for security seems like a bad idea. After all, security is all about limiting exposure and control to authorised individuals. But there are already some interesting examples, so that it may be an advantageous path for future research.

Social collaboration

There are numerous ways in which social assistance might be used to improve human interaction with technology. For example, there are applications that utilise explicit human involvement when attempting to bring older generations online might rely upon (human) social intermediaries (Blythe and Monk, 2005). At the other end of the spectrum are examples of large, complicated problem-solving efforts, such as those requiring large computations, where techniques such as distributed computation can help. One such example is the Search for Extraterrestrial Intelligence (SETI) in which idle time on people's computers is used to number crunch vast amounts of interstellar radio data (Nov et al., 2010).

File sharing and peer-to-peer networks are similar examples of social interaction and collaboration in which the lack of a (cheap) source of digital media has led to proliferation of communal media sharing networks (Good and Krekelberg, 2003). In some cases, the social interaction can help solve large challenges such as digitising old books, where computerised methods still struggle (von Ahn et al., 2008). These and other crowdsourcing applications are often driven by a desire to reduce costs (Hoffmann, 2009), though their impact on usability is not always immediately evident. Even further, such forms of human computation have their challenges, including motivating, orientating, and sustaining participation (Reeves and Sherwood, 2010). Yet it is early days, and still worth considering how such models can be applied to security challenges, and whether they would reap usability benefits.

Usable security and privacy challenges

Implementing security is easy. To implement or improve security while being usable is more difficult. For example, it would be easy to improve password security by requiring 50-character passwords subject to stringent rules. Obviously, such requirements aren't user-friendly and might actually be a detriment to security if such difficult to memorise passwords were written down and not adequately protected. Can the above interaction models be applied to security? In terms of distributing complex computations, there are already similar examples of social interaction for security. For example, distributed computational efforts have been undertaken to factor large integers in order to demonstrate the insecurity of variations of RSA, an encryption method whose security relies upon the difficulty of factoring large integers (Kleinjung et al., 2010). Similarly, attackers use distributed computation in the form of botnets in order to mount attacks such as denials of service (Abu Rajab et al., 2006). However, social methods show some potential for improved security protection as well as security attacks. Two such examples are using social interaction for authentication, and for navigating the Internet with privacy protection.

Social authentication

For many years there have been multi-control systems requiring the actions of more than one party. These are often done for critical security functions, such as launching nuclear weapons (Simon and Zurko, 1997). More advanced threshold schemes based on secret sharing require the actions of n of m individuals (Shamir, 1979). Such solutions have more recently been applied to authentication and building entry (Brainard et al., 2006) and also for online account recovery (Schechter et al., 2009) whereby an account holder registers trustees who are later involved in the recovery process. These applications require the explicit participation of other users, and for this reason have a number

of usability challenges and might be suited to niche applications. Rather than explicit participation, implicit assistance of other users based upon their previous choices and experiences might benefit users. For example Schechter et al. (2010) recently proposed a password authentication solution whereby a password choice is acceptable so long as it is not too popular. This concept removes the need for complicated password rules and relies upon a communal concept of which passwords can be used in an effort to flatten the distribution of passwords chosen, and therefore make attacks more challenging. A similar result for flattening the answers to challenge questions was highlighted by Bonneau et al. (2010). While this concept certainly raises its own usability challenges (for example what constructive feedback is returned to a user if their password choice is rejected), it does offer a new way of thinking for social authentication.

Social navigation

Collaborative solutions for privacy protection on the web have been available for many years, with a focus on anonymous web browsing (Dingledine et al., 2004), and have more recently been subjected to usability testing (Clark et al., 2007). Such methods require passive participation from other members of a network, who aid in the private routing of network packets, thereby allowing users to surf the web anonymously. Alternative solutions look to improve user decision-making based upon the experiences of others, and are referred to as social navigation (Goecks et al., 2009; Besmer et al., 2010). Recent results suggest positive changes in user behaviour resulting from additional community information, such as which personal information to share about yourself with others on a social network, though only if that information is augmented with strong visual cues. Such solutions are similar to those based upon reputation, which itself offers another potential area for improving security and usability performance, and moving beyond current challenges (Hogg, 2009).

Social security tomorrow

It is perhaps ironic that we are looking to leverage human interaction for improved security and usability, while at the same time a computer was recently crowned the new Jeopardy champion (Ferrucci, 2010). And even from the early results above we see that social interaction is not a panacea for usable security. Yet with a goal of ensuring that users are well informed when making security decisions, social interaction offers a fruitful path for future research.

REFERENCES

Rajab, M.A., Zarfoss, J., Monrose, F. and Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, IMC '06, 41–52. New York: ACM.

Adams, A. and Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM*, **42**:12, 40–46.

Besmer, A., Watson, J. and Lipford, H.R. (2010). The impact of social navigation on privacy policy configuration. In Lorrie Faith Cranor, editor, *SOUPS*, volume 485 of ACM International Conference Proceeding Series. ACM.

Blythe, M. and Monk, A. (2005). Net neighbours: adapting HCI methods to cross the digital divide. *Interacting with Computers*, 17, **3**:1, 35–56.

Bonneau, J., Just, M. and Matthews, G. (2010). What's in a name? In Radu Sion, editor, *Financial Cryptography*, volume 6052 of Lecture Notes in Computer Science, 98–113. Springer.

Brainard, J.G., Juels, A., Rivest, R.L., Szydlo, M. and Yung, M. (2006). Fourth-factor authentication: somebody you know. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM Conference on Computer and Communications Security*, 168–178. ACM.

Clark, J., van Oorschot, P.C. and Adams, C. (2007). Usability of anonymous web browsing: an examination of tor interfaces and deployability. In Lorrie Faith Cranor, editor, *SOUPS*, volume 229 of ACM International Conference Proceeding Series, 41–51. ACM.

Cranor, L.F. and Garfinkel, S. (2005). *Security and Usability: Designing Secure Systems that People will Use*. O'Reilly.

Dingledine, R., Mathewson, N. and Syverson, P.F. (2004). Tor: The second-generation onion router. In *USENIX Security Symposium*, 303–320.

Ferrucci, D. (2010). Build watson: an overview of deepqa for the jeopardy! challenge. In *Proceedings of the 19th international conference on Parallel architectures and compilation techniques*, PACT' 10, 1–2. New York: ACM.

Goecks, J., Edwards, W.K. and Mynatt, E.D. (2009). Challenges in supporting end-user privacy and security management with social navigation. In Lorrie Faith Cranor, editor, *SOUPS*, ACM International Conference Proceeding Series. ACM.

Good, N.S. and Krekelberg, A. (2003). Usability and privacy: a study of kazaa p2p file-sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI' 03, 137–144. New York: ACM.

Hoffmann, L. (2009). Crowd control. *Communications of the ACM*, 52, 16–17.

Hogg, T. (2009). Security challenges for reputation mechanisms using online social networks. In *Proceedings of the 2nd ACM workshop on Security and artificial intelligence*, AISec' 09, 31–34.

Kleinjung, T., Aoki, K., Franke, J., Lenstra, A.K., Thome, E., Bos, J.W., Gaudry, P., Kruppa, A., Montgomery, P.L., Osvik, D.A., te Riele, H.J.J., Timofeev, A. and Zimmermann, P. (2010). Factorization of a 768-bit rsa modulus. In Tal Rabin, editor, *CRYPTO*, volume 6223 of Lecture Notes in Computer Science, 333–350. Springer.

Nov, O., Anderson, D. and Arazy, O. (2010). Volunteer computing: a model of the factors determining contribution to community-based scientific research. In *Proceedings of the 19th international conference on World wide web*, WWW' 10, 741–750. New York: ACM.

Reeves, S. and Sherwood, S. (2010). Five design challenges for human computation. In *Proceedings of the 6th Nordic Conference on Human–Computer Interaction: Extending Boundaries*, NordiCHI' 10, 383–392. New York: ACM.

Schechter, S.E., Herley, C. and Mitzenmacher, M. (2010). Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks. In *Proceedings of the 5th Usenix Workshop on Hot Topics in Security*, Hotsec' 10. Usenix.

Schechter, S.E., Egelman, S. and Reeder, R.W. (2009). It's not what you know, but who you know: a social approach to last-resort authentication. In Dan R. Olsen Jr., Richard B. Arthur, Ken Hinckley, Meredith Ringel Morris, Scott E. Hudson, and Saul Greenberg, editors, *CHI*, 1983–1992. ACM.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, **22**:11, 612–613.

Simon, R.T. and Zurko, M.E. (1997). Separation of duty in role-based environments. In *Computer Security Foundations 10th Workshop Proceedings*, 183–194.

von Ahn, L., Maurer, B., McMillen, C., Abraham, D. and Blum, M. (2008). recaptcha: Human-based character recognition via web security measures. *Science*, **321**:5895, 1465–1468.

WHO IS THE ENEMY?

Karen Renaud and **Robbie Simpson** of Glasgow University ask whether users are still the enemy a dozen years down the road.

Are users still the enemy?

In 1999 Adams and Sasse published a paper titled 'Users are not the enemy', which pointed out that computer users could not cope with the demands of security policies, specifically maintenance of multiple different passwords. They enumerated some *coping skills* deployed by computer users to deal with unreasonable demands posed by multiple regularly changing passwords. They urged security professionals to stop considering the user as the enemy and rather to give due consideration to the difficulties they experience in maintaining their passwords.

Adams and Sasse's paper is considered a seminal paper in the field of usable security. It can reasonably be said to have launched a new and thriving research area. The question we are posing here is: has it made an impact on how users are viewed by security specialists? To answer this we carried out a survey in a large health board and with a group of students, asking them pertinent questions related to their use of passwords.

Does password advice improve secure behaviour?

A survey was carried out with 328 employees of a large UK health board, and with 57 students at a UK university to investigate this question.

The NHS takes information security extremely seriously since the data they hold is very sensitive. Their data breaches are gleefully seized upon and trumpeted by the tabloid press, which leads to embarrassment and dismissals in many cases. They have well-established mechanisms for ensuring information security and one could expect their compliance levels to be superior given the context. The board's password policy states the following with respect to password management:

- Passwords must not normally be written down.
- Passwords must not relate to the system being accessed.
- Passwords must not relate to the user.
- Passwords should be different for each system accessed.
- Re-use of passwords is not allowed.

These, with the exception of the last, relate to well-known coping skills people employ when confronted by too many passwords (Adams 1999). There is nothing unusual about these directives; from a security perspective they are reasonable and serve to help guarantee accountability and non-repudiation. However, as Adams and Sasse pointed out in 1999, they are unworkable in the face of multiple passwords. Our survey, carried out a dozen years later, sought to determine how much impact this kind of policy was having on the behaviours reported in 1999, when security policies were used in only a minority of organisations. There is great faith in training and awareness in the information security world. As a consequence, the NHS invests a great deal of time and effort into training and awareness. This survey gauged the effects of the policies, combined with the training efforts, on employee behaviour.

The students were surveyed to determine whether the 'modern generation' were any better at coping with the password demands of multiple systems. Students sign a 'conditions of use' form before being allowed to access University computers but this does not include any advice about password use.

Results suggest that users don't always follow advice given

A number of coping skills were mentioned and respondents were asked whether they used any of them. The percentages who responded in the affirmative are shown in Table 1.

Of the 109 employee respondents who wrote down their passwords, two added a note to say that the passwords were recorded securely and four said that they stored the password in a Word document. One of these said they stored the file in an obscure location,

Table 1		
Technique	Employee %	Student %
Write them down	33	38
Reuse passwords on multiple systems	63	61
Use the system name	10	12
Use their own name	19	27
Use the month and year, or birthday	7	30

Table 2		
Technique	Number employees	Number students
Strength from letters and numbers	153	55
Something personal	52	30
Something obscure or secret	6	1

which would not be obvious to others. One stored the passwords on their mobile phone. In stark contrast 68% of the students said they encrypted their password records.

Respondents also volunteered their own pet coping techniques in the provided 'empty' field – see Table 2. Two employee respondents were philosophical, commenting:

- Try to remember them, use things that are likely to be remembered easily;
- Use different ones: frequently have to phone someone to find out what they are if not used for a while – time consuming.

One would expect to see fewer password coping techniques being used by the employees for two reasons: the first is that they have a policy which explicitly forbids these techniques and the second is that they can be disciplined for non-compliance. Yet the figures are remarkably similar across the two groups.

Over 10 years on and user behaviour has not changed significantly

The unfortunate conclusion is that neither Adams and Sasse's paper nor all the other work published by the usable security researchers has made any difference so far. Security professionals still compose and attempt to enforce unworkable password policies. They do this because from their perspective these restrictions are necessary and required. The fact that users cannot and will not abide by their edicts is an unfortunate fact of life. Their response to this problem is to run courses to train users and to raise awareness of security issues. So the user *is* still considered the enemy, heedlessly compromising information security.

As in 1999, there still appear to be two camps: the security professionals on the one side requiring compliance with their directives and the ordinary users, unable to comply. This kind of stand-off has been seen in other areas too. Previously there was a distinct stand-off between health professionals and patients, with medics requiring compliance with their instructions, and patients failing to comply for a variety of reasons.

Health professionals have, by and large, realised the folly of issuing edicts (Robinson et al., 2008; Feste and Anderson, 1995). Their approach now is to empower and support rather than requiring blind and unquestioning compliance. They have come to understand the importance of the patient as an autonomous being, playing an active role in his or her own health maintenance. They persuade rather than instruct.

To use these findings to inform practice in information security we have to consider that there might well be a fatal flaw in the way the directives in security policies are currently formulated. Martins (2005) posits that:

> knowledge itself becomes something discrete and unified, to be passed on or delivered via an authority, rather than something dynamic, contextually based, and produced through meaning-making practices.

Generic rules are often unworkable within particular contexts and security specialists need to find a way of accommodating differing contexts to move towards empowerment rather than control.

It is time for security professionals to learn from professionals in other areas. There is a need to move away from the 'do as you are told' stance. The evidence clearly shows that it does not work and is counter-productive. It would be so much better to accommodate human frailties, to give users the tools to support them in behaving securely, to acknowledge the valuable role that they can play in securing information.

For the surveyed organisation it might well be time to issue employees with a password storage application. This would allow them to record their passwords, but ensure that they do this securely. The student group are clearly already doing this, intuitively adopting the most effective coping strategy. Hence our recommendation is for an approach which *empowers* rather than merely exercises control.

Time for a new approach

Having concluded that users are still the enemy, one has to ask why this is so. The answer appears to be that we are still clinging to the unworkable practices of the past, i.e. requiring unquestioning compliance to generic and often unworkable directives.

Here we argue for a middle ground, an empowering of end-users rather than the currently imposed unrealistic demands. We also argue for a more nuanced approach, an approach which considers the end-user's context and limitations. The only road forward is one where we work together towards an equitable solution, not one where one group imposes, another disposes, and information security is the ultimate loser.

REFERENCES

Adams, A. and Sasse, M.A. (1999). Users are not the enemy. *Communications of the ACM*, **42**:12, December 1999, 40–46.

Feste, C. and Anderson, R.M. (1995). Empowerment: from philosophy to practice. *Patient Education and Counseling*, **26**,139–144.

Martins, D.S. (2005). Compliance Rhetoric and the Impoverishment of Context. *Communication Theory*, **15**:1, 59–77.

Robinson, L.A., Emmons, K.M., Moolchan, E.T. and Ostroff, J.S. (2008). Developing Smoking Cessation Programs for Chronically Ill Teens: Lessons Learned from Research with Healthy Adolescent Smokers. *Journal of Pediatric Psychology*, **33**:2, 133–144.

SECURITY FOR HUMANS

The researchers at Cylab Usable Privacy and Security Group are the founders of a community of researchers in this field. Here **Lorrie Faith Cranor** summarises the research that led to the human-in-the-loop framework.

There is growing recognition that privacy and security failures are often the results of cognitive and behavioural biases and human errors. Many of these failures can be attributed to poorly designed user interfaces or secure systems that have not been built around the needs and skills of their human operators. Thus, usable privacy and security has emerged recently as a strategic research area.

In our work at the CyLab Usable Privacy and Security (CUPS) Laboratory at Carnegie Mellon University, we seek ways to design security solutions less reliant on humans for security-critical functions, and to build secure systems that are more resilient to human faults and less prone to human error. We are researching ways to make secure systems more understandable to non-experts and to educate non-experts in basic computer security concepts.

The human in the loop

When secure systems rely on humans to perform security-critical functions, threats to system security include not only malicious attackers, but also non-malicious humans who don't understand when or how to perform security-related tasks, and humans who are unmotivated to perform security-related tasks (Cranor, 2008). To design a system that is both usable and secure requires simultaneous consideration of attackers and legitimate users, as well as the realisation that a poorly designed system turns unwitting legitimate users into major sources of vulnerability.

We have developed a framework that provides a systematic approach to considering human factors when designing secure systems. This human-in-the-loop framework (shown in the diagram opposite) is based on a communications processing model in which a security communication (e.g. a pop-up warning, corporate security policy notice, or a newspaper article) is sent to a human receiver in order to produce a behaviour. Along the way the communication may be subject to various impediments. The human receiver must notice the communication, pay attention to it, and comprehend it before he or she is likely to respond. The receiver's personal characteristics, beliefs, motivation, and capabilities will play a role in determining what behaviour results (Cranor, 2008).

Secure systems designers can use the human-in-the-loop framework in the design process or to help determine the cause of problems in implemented systems. Designers should first identify all of the tasks that the secure system relies on humans to perform. They should then consider the feasibility of automating some of these tasks or changing the system design so they are not necessary. They can use the human-in-the-loop framework to identify places where failures are likely to occur, and conduct user studies to determine how frequently they occur. Once designers determine where failures are most likely, they can consider further system design changes to mitigate these problems (Cranor, 2008).

Protecting users from phishing attacks

Phishing is an example of a security attack that exploits human limitations rather than system limitations. We've done a number of projects in our lab to first better understand why people fall for phishing attacks, and then to understand how they respond to anti-phishing warnings, how to improve these warnings, and how to best educate users to avoid falling for these attacks. Our initial studies revealed that people are largely unaware of how phishing works and what they can do to protect themselves. They often adopt counter-productive strategies such as judging websites based on how professional they look and whether or not they include familiar logos (Downes et al., 2006). We learned that we need to teach people how easy it is for an attacker to copy logos and entire websites, and how to use URLs to determine what website they are on. In a study we conducted on phishing warnings built into web browsers, we learned that these warnings are often mistaken for less severe warnings and that some people fail to realise that not only is the website suspicious, but also the email that contained the link they clicked on to arrive at that website (Egelman et al., 2008).

One of the keys to protecting users from phishing attacks is user education. However, it is difficult to convince users to spend time learning about computer security. We developed an interactive game called Anti-Phishing Phil that teaches users about parsing URLs and identifying phishing attacks while they play a fun game. Our scientific studies demonstrated the effectiveness of this approach (Sheng et al., 2007). We also developed a training system called PhishGuru in which companies send simulated phishing messages to their employees, and when the employees take the bait, they are shown a comic strip with an anti-phishing educational message. We conducted a study with faculty and students at our university and demonstrated that those trained with PhishGuru were significantly less likely to fall for subsequent phishing attacks (Kumaraguru et al., 2009). Anti-Phishing Phil and PhishGuru are now being sold by Wombat Security Technologies, and are being used by organisations around the world to train their employees and customers.

Computer security warning dialogues

Pop-up warning dialogues are used in computer software to warn users about potential security hazards. However, users often ignore these warnings, making them an ineffective form of protection. Indeed, as with physical-world warnings, computer security warnings should be used as a last line of defence after first attempting to design out or guard against hazards. Where it is possible for computers to

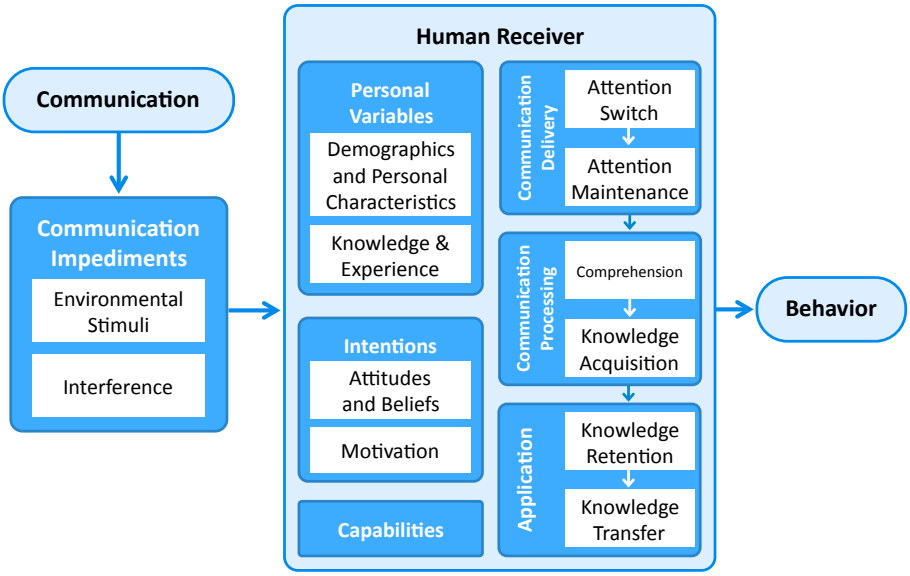
detect and guard against hazards with high levels of accuracy, it may be possible to eliminate warnings altogether. In other cases, computers can take advantage of available information to determine the level of risk posed by a potential hazard. When the risk is determined to be extremely low, it may be better not to bother displaying a warning. However, in some cases the level of risk depends on contextual information that is known to the user but not the computer. For example, a user may know whether a particular attachment is expected or whether he or she is attempting to visit the website of a bank. In cases like this, a warning dialogue may be used to assist the user in interpreting this context and deciding how to proceed.

Unfortunately, many of the computer security warning dialogues commonly in use today are ineffective. For example, we conducted a study of web browser certificate warnings and found that users frequently ignored them, even when they appeared on the login page for the user's own online bank account. We applied a number of techniques to improve these warnings and were able to reduce the number of users who ignored them. However, even in the best case, far too many users ignored our improved warnings. Other approaches are needed to better remove or guard against attacks that result in certificate warnings, since these warnings are failing to protect users (Sunshine et al., 2009).

In ongoing work, we are developing and testing guidelines to improve computer security warning dialogues and reduce the frequency of their occurrence. We are evaluating ways to succinctly and clearly communicate with users about the risk, to motivate them to pay attention to the warning, and to help them determine which course of action to take.

Making passwords usable and secure

Passwords are, perhaps, the most widely used and widely disliked computer security mechanism today. Text passwords were a reasonable approach when each user had only one or a small number of accounts. But now that typical users have dozens of accounts, good password security practices demand they create and remember dozens of unique, complicated passwords. Unfortunately, this is beyond the cognitive ability of most humans. Therefore, people use a variety of coping mechanisms, including re-using the same password across multiple systems, choosing predictable passwords, and writing their passwords down. While there are some more secure approaches such as password management software, these too pose challenges to usability and convenience. In addition, we have yet to see text password alternatives that adequately address both security and usability without adding additional implementation costs.



Increasingly system administrators are implementing password policies that require users to pick passwords that contain multiple character classes, such as symbols, numbers, and capital letters. But until recently, there has been little empirical data on the effectiveness of such policies. We have conducted a series of studies to determine how various password policies impact the entropy and guessability of passwords users create, as well as the usability of the password system (including ease of password creation and memorability). We have found that users do find complicated password requirements burdensome, and that their use tends to increase the use of coping mechanisms. While our work is still ongoing, our preliminary results suggest that policies that require longer passwords may result in more password entropy with less user burden than policies that require multiple character classes (Komanduri, 2011; Shay, 2010).

Originally published in the February 2011 issue of *The Innovator*, BITS Financial Services Roundtable.

REFERENCES

Cranor, L. (2008). A Framework for Reasoning About the Human in the Loop. *Usability, Psychology and Security 2008*. www.usenix.org/events/upsec08/tech/full_papers/cranor/cranor.pdf

Downs, J., Holbrook, M. and Cranor, L. (2006). Decision Strategies and Susceptibility to Phishing. In *Proceedings of the 2006 Symposium On Usable Privacy and Security*, 12–14 July 2006, Pittsburgh, PA. cups.cs.cmu.edu/soups/2006/proceedings/p79_downs.pdf

Egelman, S., Cranor, L. and Hong, J. (2008). You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. *CHI 2008*. doi.acm.org/10.1145/1357054.1357219

Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L. and Egelman, S. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. *CHI2011*.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A. and Pham, T. (2009). School of Phish: A Real-Word Evaluation of Anti-Phishing Training. *SOUPS 2009*. cups.cs.cmu.edu/soups/2009/proceedings/a3-kumaraguru.pdf

Shay, R., Komanduri, S., Kelley, P., Leon, P., Mazurek, M., Bauer, L., Christin, N. and Cranor, L. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviors. *SOUPS 2010*. cups.cs.cmu.edu/soups/2010/proceedings/a2_shay.pdf

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 2007 Symposium On Usable Privacy and Security*, Pittsburgh, PA, July 18–20, 2007. cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf

Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. and Cranor, L. (2009). Crying Wolf: An Empirical Study of SSL Warning Effectiveness. *USENIX Security 2009*. lorrie.cranor.org/pubs/sslwarnings.pdf

SEEKING THE PHILOSOPHER'S STONE

Ivan Fléchais and **Shamal Faily** of Oxford University Computing Laboratory go in search of the elusive alchemy of systems that are both usable and secure.

Moving usable privacy and security forward

> … might there exist a remarkable analogy between this usable and secure system and the ancient alchemists' philosopher's stone?
>
> Auguste Kerckhoffs
> *La Cryptographie Militaire*, 1883

This article describes the unique challenges facing usable security research and design, and introduces three proposals for addressing these. For all intents and purposes security design is currently a craft, where quality is dependent on individuals and their ability, rather than on principles and engineering.

However, the wide variety of different skills necessary to design secure and usable systems is unlikely to be mastered by many individuals, requiring an unlikely combination of insight and education.

Psychology, economics and cryptography have very little in common, and yet all have a role to play in the field of usable security. To address these concerns, three proposals are presented here:

- to adopt a principled design framework for usable security and privacy,
- to support a research environment where skills and knowledge can be pooled and shared, and
- to guide and inform the principles that underpin the educational curriculum of future security engineers and researchers.

Since 1883 the need for usable security has been recognised

The quest for secure and usable systems is neither new nor complete. Even in 1883, Auguste Kerckhoffs was lamenting the failures of the French army to employ a usable and secure cryptographic system (Kerckhoffs, 1883). While this treatise is known for expressing one of the most famous cryptographic principles – that a cryptographic algorithm should not depend on secrecy for its strength – the sixth principle also states:

> **Finally, it is necessary, given the circumstances that command its application, that the (crypto) system be simple to use, requiring neither mental strain, nor the knowledge of a long series of rules to observe.**

The world has now moved on. Issues of security and usability are no longer the province of military cryptographers but of software developers, system administrators, and the user community.

Nevertheless, progress in usable security research and design has been slow, due in part to the need to master a large amount of (usually) mutually exclusive, yet necessary, skill and knowledge. To quote from Ross Anderson, 'the security engineer needs to understand basic economics as well as the basics of crypto, protocols, access controls, and psychology' (Anderson, 2008). Addressing

The quest for secure and usable systems is neither new nor complete.

this fundamental dilemma is necessary if the field of usable privacy and security is to deliver on its promises.

The following sections describe three proposals for the field of usable security and privacy, aimed at fostering a sound design, research and educational foundation.

Adopt a design approach

Relying on individuals to master the many different fields of knowledge necessary for usable security and privacy research is not an option when practitioners need to build systems. Design frameworks are the only means whereby different skills can be utilised and harmonised for the common purpose of building a usable secure system.

A forum is required to solicit and provide a venue for research in usable security design, and encourage existing work to formulate and discuss human-centered security engineering principles and practices.

Support an interdisciplinary research environment

Usable security and privacy is a multidisciplinary problem, and supporting a research environment where these disciplines can come together and inform one another is not only desirable but necessary. Like SOUPS (discussed in the article by Lorrie Cranor), a European network could contribute to this research environment by both providing a venue for disseminating research findings, and forging new connections between researchers and industry that last beyond an annual event. The purpose behind this network would be to facilitate the sharing of knowledge, to identify areas of expertise and to encourage collaboration in the pursuit of new research.

Some practical ideas for establishing this network could include:

- the creation of a social network of interested parties,
- a centrally accessible and persistent resource for research knowledge (including experimental designs, research methodologies, questionnaires, lists of individuals and institutions with specific expertise in relevant techniques or tools, sources of research funding and the means for groups looking to collaborate on new research projects to identify and approach other partners),
- an annual meeting at a conference, perhaps its own conference to keep the momentum going and provide an approachable venue for people who might be interested in joining.

Engage with security education

There are two aspects to engaging with security education: the first consists of providing useful educational material, perhaps in the form of podcasts or tutorials; the second aims at informing, engaging and shaping different security educational curricula.

- The creation of useful educational material is important to further the cause of usable privacy and security. Disseminating usable security and privacy know-how is predicated on this. Running tutorials or seminars at conferences is one means of doing so; another proposal would be to run a DesignFest for usable security and privacy – an activity whereby attendees would sharpen their design skills by working on real usable security problems with other participants with different backgrounds and expertise. This type of approach has proven effective and engaging at other venues such as OOPSLA, and provides attendees with a different kind of learning experience.
- Engaging with existing educational curricula requires a clear understanding of the necessary knowledge, skills and techniques that underpin usable security and privacy. Further research is needed to ascertain what these are, and how to best integrate these into the wider security arena, and a European network would be an ideal venue for this.

Conclusions

Researchers in the field of usable privacy and security currently have the opportunity to re-shape their field of research in order to address current weaknesses. By channelling efforts towards supporting engineering approaches, multidisciplinary research and security education, a European network could provide a significant European and international focus for furthering the science of usable privacy and security.

ivan.flechais@comlab.ox.ac.uk
shamal.faiiy@comlab.ox.ac.uk

REFERENCES

Anderson, R. (2008). *Security engineering: a guide to building dependable distributed systems*. 2nd edition. Indianapolis, IN: Wiley

Faily, S. and Fléchais, I. (2010). A Meta-Model for Usable Secure Requirements Engineering. In *Software Engineering for Secure Systems*, 2010, SESS '10, 126–135. IEEE Computer Society Press.

Faily, S. and Fléchais, I. (2010a). Barry is not the weakest link: Eliciting Secure System Requirements with Personas. In *BCS HCI2010: Proceedings of the 2010 British Computer Society Conference on Human–Computer Interaction*.

Faily, S. and Fléchais, I. (2010b). The secret lives of assumptions: Developing and refining assumption personas for secure system design. In *HCSE2010: Proceedings of the 3rd Conference on Human-Centered Software Engineering*, 111–118. Springer.

Faily, S. and Fléchais, I. (2010c). Towards tool-support for Usable Secure Requirements Engineering with CAIRIS. *International Journal of Secure Software Engineering*, 1:3, 57–71.

Fléchais, I. (2005). *Designing Secure and Usable Systems*. PhD thesis, University College London.

Fléchais, I., Sasse, M.A. and Hailes, S.M.V. (2003). Bringing security home: a process for Developing secure and usable systems. In *NSPW '03: Proceedings of the 2003 workshop on New security paradigms*, 49–57. New York: ACM.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2009). Usability and security of out-of-band channels in secure device pairing protocols. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010a). Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions, chapter *Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions*.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010b). Security and usability: Analysis and evaluation. In *Availability, Reliability and Security*. ARES 10.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010c). Two heads are better than one: Security and usability of device associations in group scenarios. In *Proceedings of the 2010 Symposium on Usable Privacy and Security* (SOUPS 2010).

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, 5–38.

WHO KNOWS ABOUT ME?

Linda Little, **Pam Briggs** and **Lynne Coventry**, Northumbria University, discuss people's willingness to discolose different types of information to different people and highlight the need for tools to help people manage their privacy preferences

How private are people

The disclosure of highly sensitive personal information is happening on an unprecedented scale, raising important questions about user preferences in respect of privacy, defined here as 'an individual right to determine how, when and to what extent information about the self will be released to another person' [11]. New privacy challenges are inevitable with the growth of online interaction [7]. For example, users wishing to sign up for an online product or service or wishing to simply join a group are typically asked to provide a significant profile of personal data on enrolment and are, thereafter, subject to a subtle data-collection process in respect of personal choices and preferences.

Unsurprisingly, then, a research agenda has grown up around understanding disclosure patterns and privacy preferences [3], in part driven by the perceived need to automate such disclosure processes and preferences and in part driven by the rather worrying observation that, in the face of known privacy risks, users seem willing to give away personal identity information very cheaply [4].

Internet users who hold privacy in high regard can recognise not only the costs, but also the potential benefits to information disclosure [3]. Researchers have recently begun to understand privacy management in terms of the costs and benefits of informational trade-offs, and a new study of 'privacy economics' has emerged, where privacy benefits can include better access to relevant information and targeted sales advice, while privacy costs can include identity threats and physical vulnerabilities dependent upon location disclosures, e.g. [1]. As information exchange becomes more ubiquitous, responsibility for the calculation of costs and benefits for each single exchange can become too much for any individual, with the result that a significant research effort is being targeted at the construction of automated 'trust agents' or 'privacy wizards, capable of managing disclosure decisions seamlessly [2].

Effective risk management is conceptually possible in the privacy domain; however, many users act as if they are either unaware of the risks and consequences of revealing too much personal information in online environments [12] or as if they simply don't care [3]. Indeed, the privacy literature is peppered with examples of users who vouchsafe the importance of privacy protection while, at the same time, eschew privacy protection behaviours [5].

Nowhere is this more obvious than on social networking sites. For example, Facebook users seem very willing to disclose highly sensitive information in relation to their personal identity and lifestyle [4, 6]. Real names, pictures, dates of birth, telephone numbers, employment status and even physical addresses have all been recorded as being openly accessible by strangers, despite the fact that such personal disclosure can lead to identity theft and more disturbing outcomes such as stalking [9].

Subsequent studies of different student communities, e.g. [8], have shown very similar patterns of high levels of personal disclosure. In the Tufekci study [10], for example, two-thirds of students from a sample of 601 disclosed their sexual orientation and relationship status, half disclosed their political and religious orientation and almost a third gave out their phone number.

Our study sought to look in more detail at people's disclosure patterns. In this article, we present a preliminary analysis of a survey of over 1000 people, delivered via Zoomerang, focusing on age-related trends in disclosure preferences. Our rationale for this focus is that, while the willingness of young people to disclose personal data about themselves is well established [10], other possible age-related patterns have been left unexplored.

Using a disclosure grid to map information to recipient

Participants were presented with a 'disclosure grid' that asked them to consider a range of different pieces of information set against a range of different information recipients. In each cell of the grid they were asked to rate on a scale of 1–5 how happy they would be to reveal this information to that individual or group. For the purpose of the analysis, information was collapsed into four main groups:

1 Personal identity: name, date of birth;
2 Health: medical history, family medical history, allergies, current medication, genetic disorders, GP visits;

3 Lifestyle: lifestyle, shopping habits, employment status;
4 Financial: financial details, current bank balance.

Information recipient was also collapsed into four main types:

1 Health professional: doctor, hospital consultant;
2 Family/friend: partner, family member, friend;
3 Work acquaintance: employer, work colleague;
4 External companies: private company, government agency, financial institution.

Results

Participant responses were divided into three age groups (>35, 36–55, 56< years) and multivariate ANOVAs were conducted to find any differences between the groups in terms of how happy they were to disclose different types of personal information.

Personal Identity information

The results show, firstly, an extreme willingness to disclose personal identity data. There were no significant differences between age groups for happiness to disclose personal identity information to either health professionals or family/friends. However, participants aged 36–55 feel significantly less comfortable disclosing personal identity information to external companies or work acquaintances than the younger and older age groups.

Health information

The results show there were no significant differences between age groups for happiness to disclose health information to any of the groups.

Lifestyle information

The results show there were no significant differences between groups for happiness to disclose lifestyle information to either health professionals, work acquaintances or external companies. However, participants aged 36–55 feel significantly less comfortable disclosing lifestyle information to family/friends than the younger and older age groups.

Financial information

The results show there were no significant differences between groups for happiness to disclose financial information to either health professionals or family/friends. However participants aged over 56 feel significantly less comfortable disclosing financial information to external companies in comparison to the under 35s.

Discussion

Overwhelmingly, our first observation should be the remarkable willingness of our participants to disclose identity information in comparison with other information types. The data suggests we have become rather blasé in the disclosure of names and dates of birth and have reconciled ourselves to giving up such information as the first bargaining chip in an information exchange. Our second point concerns age. Data suggests a dip in willingness to disclose information during middle age, the notable exception to this pattern being the disclosure of financial information.

Older adults have told us they're happier to share personal information than those in middle age (aged 36–55). Why might this be? One interpretation is that, as we enter middle age, we become more aware of the implications of data sharing – we understand the ways in which personal data has value. Earlier we discussed the kinds of cost–benefit analyses that any individual may undertake in weighing up a disclosure decision. As we engage more fully with society, we come to realise both costs and benefits more fully and also realise that we may have more to lose – in terms of our status in society and specific monetary issues such as salary and insurance privileges. Later, as we move into our sixties and beyond, we regain a willingness to disclose information in all but the financial domain.

Next steps

We are well aware that, in this work-in-progress, we are limited to self-report data; however, this study forms part of a series of studies in which we seek to combine the results from such surveys with observational studies of real data sharing in order to better understand both stated preferences and actual behaviours.

What we would argue here is that our understanding of the way privacy concerns are developed and shaped over time, and the way that such concerns come to shape behaviour is as yet very poorly understood. Furthermore, this paucity of understanding is reflected in the limited range of technological solutions available. Better tools are needed to capture and understand privacy preferences and it is these that will be the focus of our future work in this area.

REFERENCES

1 Ahern, S., Eckles, D., Good, N.S., King, S., Naaman, M. and Nair, R. (2007). *Over-exposed?: privacy patterns and considerations in online and mobile photo sharing*, SIGCHI conference on Human factors in computing systems, San Jose, California, USA.

2 Gross, R. and Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*.

3 Guha, S., Tang, K. and Francis, P. (2008). NOYB: Privacy in Online Social Networks. *WOSN'08*, August 18, 2008, Seattle, Washington, USA. 49–54.

4 Leathern, R. (2002). *Online Privacy: Managing Complexity to Realize Marketing Benefits*. www.forrester.com.

5 Lederer, S., Mankoff, J., and Dey, A.K. (2003). Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03 Extended Abstracts on Human Factors in Computing Systems*, Ft. Lauderdale, Florida, USA, April 05 – 10 2003.

6 Little, L. and Briggs, P. (2009). Privacy factors for successful ubiquitous computing. International Journal of E-Business Research, **5**:2, 1–20.

7 Olson, J., Grudin, J. and Horvitz, E. (2005). A study of preferences for sharing and privacy. *CHI 2005 extended abstracts on Human Factors in Computing Systems*.

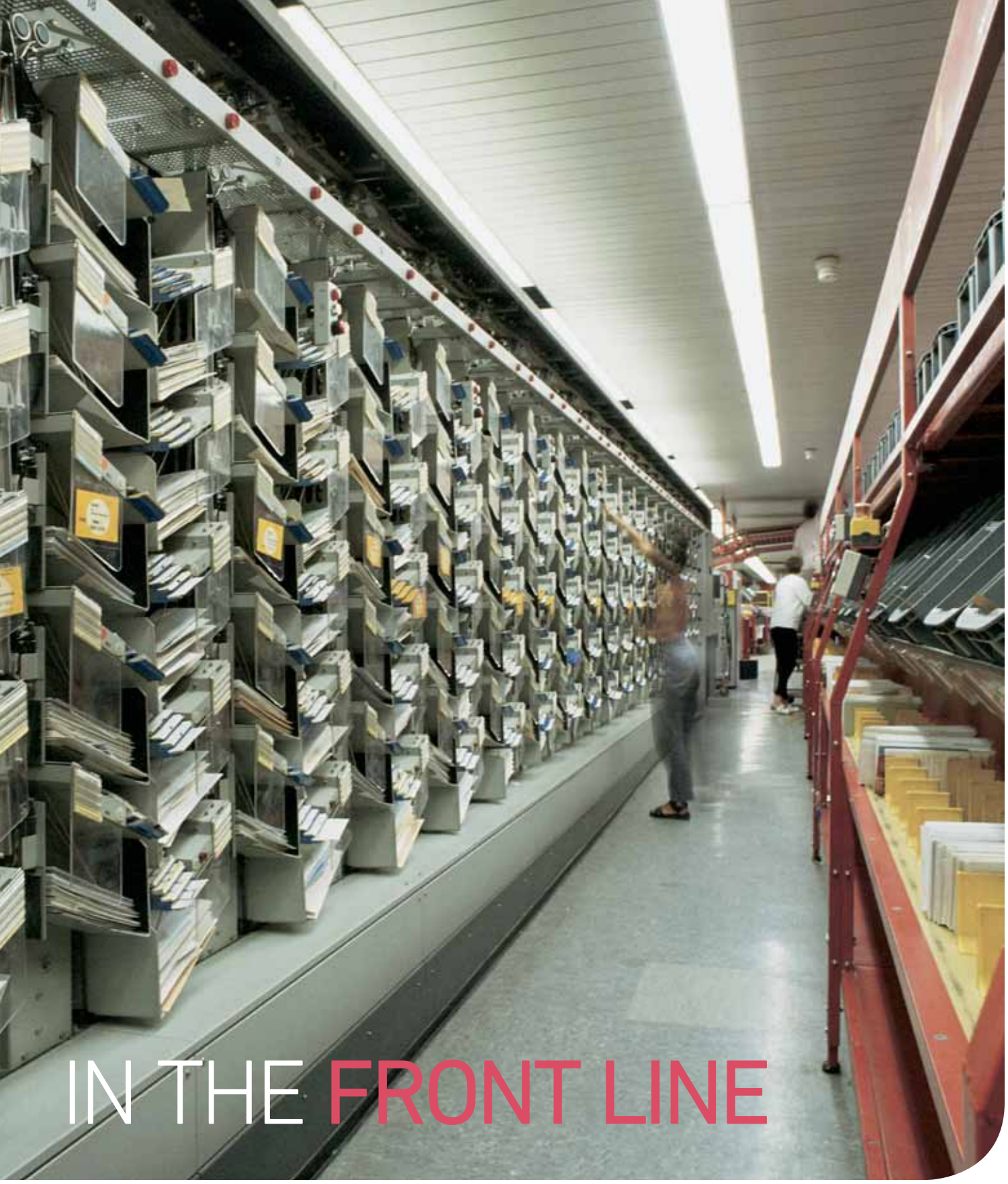
8 Schrammel, J., Koffel, C. and Tscheligi, M. (2009). How much do you tell? Information disclosure behaviour in different types of online communities. *C&T 2009*, University of Pennsylvania, USA, 275–284.

9 Strater, K. and Lipford, H.R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XX II: Culture, Creativity, Interaction*, September 01 – 05, 2008, Liverpool, United Kingdom.

10 Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society*, **28**, 20–36.

11 USACM (2006). *USACM Policy Brief: USACM Policy Recommendations on Privacy*, June 2006. usacm.acm.org/usacm/Issues/Privacy.htm.

12 Young, A.L. and Quan-Haase, A. (2009). Information revelation and Internet privacy concerns on social network sites: A case study of Facebook. In *Proceedings of the fourth international conference on Communities and Technologies*, June 25 – 27 2009, University Park, Pennsylvania, USA. ACM Press.



IN THE FRONT LINE

When, in 2007, a disk went missing containing 25 million personal records, the government and media were quick to blame the staff at HMRC, but was that fair, asks Alan Dix, Talis and Lancaster University.

Some years ago there were a series of 'security breach' stories in the UK media, the most widely reported concerning a computer disk that went astray in the post from the UK child benefits agency containing 25 million records of parents' and children's names addresses, dates of birth, bank account and national insurance details – an identity fraudsters' gold mine (BBC, 2007a). This caused concern for millions of parents, the resignation of the chair of HM Revenue and Customs (HMRC), and embarrassment in Parliament for Alistair Darling, the Chancellor of the Exchequer at the time.

The BBC produced a detailed timeline of the events (BBC, 2008) and *Computer Weekly* a slightly more technically focused account (Collins, 2007). In short, in October 2007 the National Audit Office (NAO) requested some information from HMRC. The HMRC sent a far more extensive extract than necessary on disk by courier ... which never arrived. After some internal

investigations the Metropolitan Police were called in and eventually a month after the incident the story broke when Alistair Darling made a parliamentary statement.

At the time I was approached by BBC Radio Cumbria to give a short interview about the incident, which forced me to consider the issue in a little more detail. I think they expected a more technical security angle, but obviously this was very much a human story also. Despite the gravity of the event I was shocked but not surprised. In the end if you put people in a severely time pressured, cost-controlled context mistakes will inevitably happen. So what went wrong?

Understanding and using encryption

First, but *not* most significantly, are the raw technical encryption issues. Like everyone else, I only knew what was said in public statements, but these repeatedly said the disk was password protected, but not encrypted. One of the problems on radio was how to explain this difference.

The best I could come up with was that the password-protected disk was like a briefcase with a lock – once you broke the lock the papers inside could all be easily read. In contrast the encryption was like a briefcase full of papers all in code.

But notice, the fact that I had to struggle to think of an analogy says something about the complexity of the issue. For the poor official sending the disks it could well have appeared secure. You couldn't (without specialist knowledge) access the disks without the password. And if he had encrypted them it would have looked very similar: type a password (now an encryption key, not just a key to check) and access the data.

Even when you *know* the difference, security systems are notoriously difficult to use. I know some one who used to maintain a particular mail system on her machine solely because it was the only one where she had managed to get PGP installed to digitally sign mails … and if I needed to encrypt something I think I would reach down into the UNIX crypt command or start scouring the web for a download (would I trust it?) – or more likely stick it on a disk and hope for the best.

Outsourcing expertise

One of the most telling aspects of this story was the mail from the HMRC official to the National Audit Office who had requested a far less sensitive extract of the information:

> We must make use of the data we hold and not over burden the business by asking them to run additional scans/filters that may incur a cost to the department.

This was not just a matter of internal effort, but also because producing a copy of the data with some of the fields removed would have required going to the external contractor (EDS) to produce the report. That is, due to outsourcing (to save money) Her Majesty's Revenue and Customs did not have internal IT staff who were able, or had suitable permissions or documentation, to produce what sounds like a simple database download. If there are no staff around who can extract records from a database, what hope for advising on information security?

Procedures were not followed

Repeatedly, when interviewed, Alistair Darling blamed staff at HMRC; the procedures were in place but not followed – of course nothing to do with the merging of departments, resulting staff cuts and mounting pressure at HMRC (BBC, 2007b).

As in so many stories of 'human error', for example the Zeebrugge disaster, people are put into situations where they know they need to meet certain targets, within tight time or financial constraints. The 'procedures' may be in place to make things safe or secure, but keeping to the letter of those procedures is often not possible – even if everyone knows what the procedures are. Rarely are such procedures costed and so an official or operator on the ground is forced to make, on a day-by-day basis, what are effectively strategic policy decisions: things are bound to go wrong.

In the current economic climate yet more departments and agencies are being closed and re-organised, and staff and budgets cut, creating circumstances, if anything, more strained than in 2007. Indeed, as I am writing this, news has broken of a breach at the University of York where 17,000 prospective students' names, addresses and contact numbers were released (Leyden, 2011). We can choose to spend more and have things utterly secure and safe … or choose not to. However, if we choose the latter, it is utterly unfair to blame those on the ground seeking to do the best job they can under tight circumstances.

A web version can be found at **www.alandix.com/blog/2007/12/02/fading-news-disks-astray-and-children-named**.

We can choose to spend more and have things utterly secure and safe … or choose not to.

REFERENCES

BBC (2007a). *UK's families put on fraud alert.* BBC News. news.bbc.co.uk/1/hi/uk_politics/7103566.stm

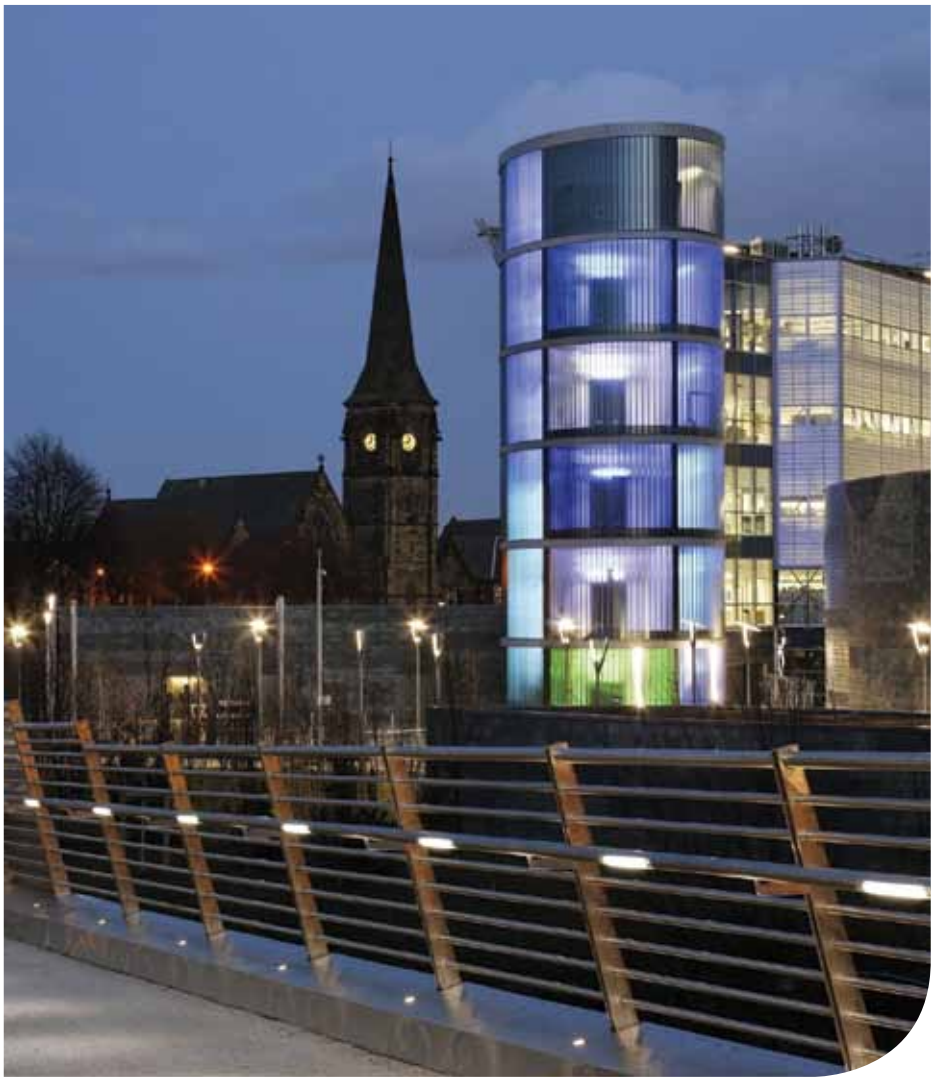
BBC (2007b). *Life inside the beleaguered HMRC.* BBC News. news.bbc.co.uk/1/hi/uk/7104395.stm

BBC (2008). *Timeline: Child benefits records loss.* BBC News. news.bbc.co.uk/1/hi/uk_politics/7104368.stm

Collins, T. (2007), Missing child benefit CDs: what went wrong, and why it would have carried on regardless. *Computer Weekly*, 21 Nov. 2007. www.computerweekly.com/Articles/2007/11/21/228217/Missing-child-benefit-CDs-what-went-wrong-and-why-it-would-have-carried-on.htm

Leyden, J. (2011). York Uni exposes students' private info. *The Register*. 16 March 2011. www.theregister.co.uk/2011/03/16/york_uni_student_data_breach

HCI2011



An inspirational event needs a setting to match ...

Programme
The HCI2011 programme is developing with a broad selection of workshops and papers. You are able to see the end result on our website,**www.hci2011.co.uk**, and we hope the offerings will entice you to make your selections and register. The early bird discount deadline is 6th May!

Health, wealth and happiness
The conference theme acted as a focus for authors and we hope you will find your interests in this theme reflected in the content of the programme; of course the more general area of HCI will also be reflected in the content.

Starting with the workshops, Siân Lindley and Peter Wild have put together a full and varied two-day programme of events.

Submission and registration
Please see the website for details on how to submit position papers. The general deadline for position papers is 1st May 2011, but check individual workshop webpages for specific information. You can also register just to attend a workshop, but only with the organisers' permission. There is no requirement to attend the main conference, but there is a reduced fee if you attend the conference as well.

Day 1: Monday 4th July 2011 (1 day)	
Workshop	Organisers
EuroHCIR2011 – The 1st European Workshop on Human–Computer Information Retrieval	Max Wilson, Tony Russell Rose, Birger Larsen, James Kalbach
HCI4WELL2 – The 2nd Workshop on HCI for Wellness: Using computers to improve mental wellness	Rich Picking, Julie Doyle, Christopher Buckingham, Stuart Cunningham, Ann Adams, Alan Newell, Paula Alexandra Silva, Paula Fraunhofer
When Words Fail: What can Music Interaction tell us about HCI?	Katie Wilkie, Rose Johnson, Simon Holland, Grégory Leplâtre
Sixth International Workshop on Ubiquitous and Collaborative Computing (iUBICOM 2011)	Rahat Iqbal, Jacques Terken, Dzmitry Aliakseyeu, Anne James
UXCF2011 – Common Curriculum Workshop for UX	Tom McEwan, John Knight, Chandra Harrison
Designing Cool	Janet Read, Daniel Fitton, Russell Beale, Linda Little

Day 2: Tuesday 5th July 2011 (1 day)	
Workshop	Organisers
HCIEd 2011 – Ten years on! What's going on?	Gavin Robert Sim, Janet Read, Lynne Coventry, Lars Oestreicher
Integrating Ambient Information into Healthcare Environments	Ruth Dalton, Nicholas Dalton, Paul Marshall, Rebecca Cain, Christoph Hölscher
Delivering User Centred Mobile Design: Commercial realities and UCD methodology	Chandra Harrison, Charlotte Magnusson, Benjamin Poppinga, Sam Medrington, Whan Stransom, Ginger Claassen
PPD11 – Workshop on Coupled Multi-display Environments (MDEs) in Classrooms	Aaron Quigley, Alan Dix, Sriram Subramanian, Stephen Brewster, Miguel A. Nacenta
Beyond Mobile Context: New and unexplored practices in mobile interaction design and research	Michael Leitner, Johann Schrammel, Manfred Tscheligi
Supporting Collaboration through Multimodal and Cross-modal Interfaces	Oussama Metatla, Nick Bryan-Kinns, Tony Stockman, Fiore Martin
The 3rd Workshop on HCI and Services	Peter Wild, Emma Pickering, John Knight, Stefan Holmlid
Health, Wealth and Identity Theft: Designing usable privacy and security mechanisms for happiness online	Lynne Coventry, Paul Dunphy, Ivan Fléchais, Tristan Henderson, Mike Just, Linda Little, Karen Renaud, Melanie Volkamer
Online Patient Experience (PEx) and its role in e-health	Sue Ziebland, Pamela Briggs, John Powell, Liz Sillence

Monday 4th July and Tuesday 5th July (2 day)	
The Second International Symposium on Culture, Creativity and Interaction Design	Shaowen Bardzell, Ann Light, Jeffrey Bardzell, Mark Blythe

Keynote speakers
Our keynote speakers are **Abigail Sellen** and **Gregory Abowd**. Abigail is a Principal Researcher at Microsoft Research, Cambridge, UK, and co-manager of Socio-Digital Systems, an interdisciplinary group with a focus on the human perspective in computing. Gregory is a Distinguished Professor in the School of Interactive Computing and the W. George Professor and Director of the Health Systems Institute at the Georgia Institute of Technology.

Exciting events
There is also the local culture to experience in the social programme of the conference. On Tuesday night we will be organising a run for the fitter amongst you and walks for the less fit or more culturally orientated. On Wednesday night there will be a drinks reception around the posters and on Thursday night our conference dinner will be hosted in the Discovery Museum. This will give you a chance to learn about the history of Newcastle.

Visit our website to view the advanced programme and to register for the conference and workshops. There is also a link to help you book accommodation.

Linda Little and **Lynne Coventry**
Conference Co-chairs

DATES FOR YOUR DIARY

Conference 4–8 July 2011

Workshop position papers deadline **1 May 2011**

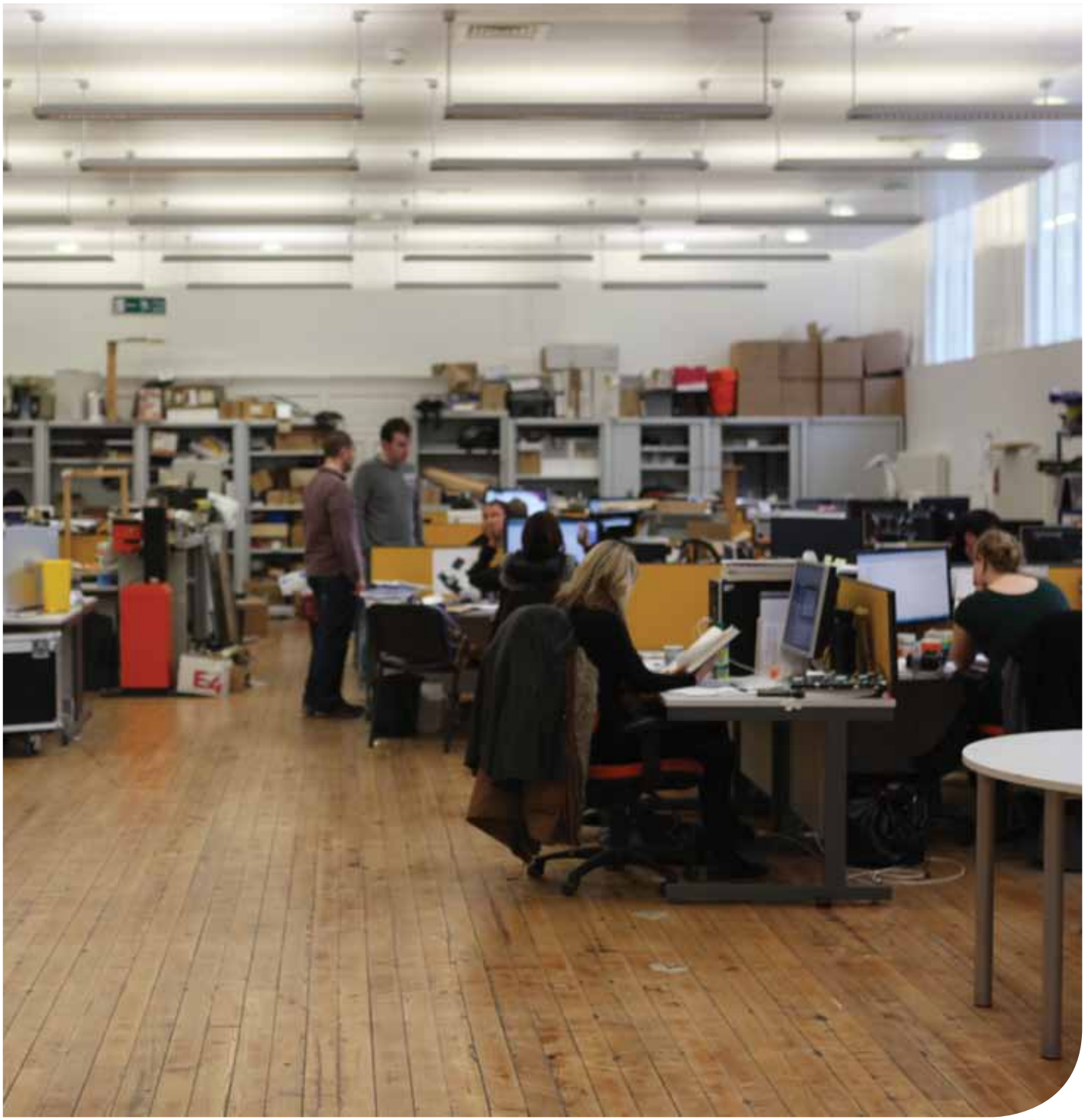
Early bird registration deadline **6 May 2011**

Venue: Northumbria University, Newcastle, UK

For more information don't forget to visit **www.hci2011.co.uk**

hci2011@northumbria.ac.uk

MY PHD



PAUL DUNPHY: USABLE AND SECURE USER AUTHENTICATION

The role of passwords has changed immeasurably since the Internet became more than an artefact of academic research. In the beginning, electronic passwords served to secure a solitary computer, in a locked room, in the building of a university or large corporation.

Today, depending on the context, their purpose is to provide high entropy resistance to guessing attacks by malicious Internet-based attackers. Websites and services demand knowledge of our identity, and alphanumeric passwords only known to us, to prove it.

Multiply this effect by a large number of websites and services and it is clear we have a password management problem. Clearly, the ubiquity of alphanumeric passwords was neither designed, nor planned, but if we could do things over again, how would we do it?

Visual authentication codes
The phrase 'A picture is worth a thousand words' is often used to refer to innate human memory for pictures against alphanumeric data (Winograd et al., 1982). This research area of visual authentication codes (Suo et al., 2005) is concerned with designing mechanisms that exploit this effect. Examples include selecting a sequence of images amongst decoys (De Angeli et al., 2005), selecting locations in a picture (Dirik et al., 2007) and making drawings (Dunphy and Yan, 2007). The goal is not to replace every alphanumeric password with a visual equivalent, but to explore to what extent visual authentication codes can alleviate the current password management problem.

Observability
My own research concerns the exploration of pertinent issues in this domain such as threat of *observation attacks* – are visual passwords more vulnerable to being stolen because of their more memorable properties? In an ATM setting users are reminded to shield input, however in practice this is at odds with maintaining personal relationships, due to the mistrust that may be signalled. To defend against this, we can either design schemes that are inherently observation resistant (e.g. one-time passwords) or augment the interaction to make it secret.

In the latter case we explored the use of an eye tracker for entry of visual passwords (Dunphy et al., 2008b). Questions that remain include: how do we even measure observability in a controlled setting? In work carried out in collaboration with Nokia Research, we took the approach of building a computer model of an attack and complementing this with the number of observations it took real people to carry out.

Sharing
Password sharing is also a more subtle issue than it may appear. The threat model online for compromising passwords has shifted away from dictionary attacks, towards users voluntarily giving passwords away in social attacks such as phishing. It is clear that we cannot prevent users from being tricked, as confidence tricksters have existed as long as humans themselves. So one desirable route is to design authentication systems where it is more difficult for the user to share their password.

Our work on 'description' (Dunphy et al., 2008) suggests that in the context of recognition-based visual passwords, strategic grouping of decoy images made it more difficult for users to identify password images given a verbal description. This is an example of how to augment an existing system to make password sharing more difficult.

We cannot prevent users from being tricked, as confidence tricksters have existed as long as humans themselves.

Barriers
Academic research often concerns itself with conceptual issues, and leaves implementation details to software engineers. However it is clear that offering insight into *deployment* is also something that is important in a security and privacy context, as this is often the aspect where an engineer might be led to make an implementation trade-off that renders a system pointless.

This is not a critique of software engineers, we should support them more by our research considering the realities of engineering such solutions, and how they might be appropriated in everyday life. The concept behind visual passwords seems quite simple but there are subtle deployment barriers such as the need for appropriate image processing techniques in order to reason automatically about the behaviour that particular images might encourage for a particular system. This is the focus of current research.

A concern I have working in this field is that due to the exploration of the design space being fairly invention-based, there are many systems that could be useful in practice whose usage is restricted due to the patent system. This is not unique to the field of user authentication, but in general the services that would benefit from some kind of novel user authentication mechanism, are not often the same organisations with the money to license patents.

Future work
For future work I am interested in exploring aspects of user experience and privacy and security mechanisms. I am currently involved in a project investigating banking for customers aged 80+, **www.cuhtec.org.uk/banking.php**, exploring the provision of financial services and technology for older users. The future of my field in general is an interesting one. The exploration of the design space has been extensively explored. Solutions such as the unlock pattern system used on Android phones show that this field is timely and relevant. However, more effort should be made to evaluate mechanisms in situ.

My PhD in Newcastle
My studies at Newcastle University started with a BSc in computing science. Newcastle itself is a great city to live in; the campus is in the city centre and the locals are well known for being a universally friendly group. The process of carrying out an undergraduate dissertation in the field of usable security and privacy was

MY PHD

Paul Dunphy is in the third year of his PhD research at Newcastle University, and is a member of the School of Computing Science in the Culture Lab. His supervisor is Professor Patrick Olivier and he has interned in the Trustworthy Communications and Identities group at the Nokia Research Centre in Helsinki, and Microsoft Research Cambridge, in the Socio-Digital Systems group.

chiefly responsible for attracting me to a career in research. I'm based in the School of Computing Science at the Culture Lab. Our theme is that of Cultural Computing and exploring systems that are designed to impact the lives of people and be appropriated. This resonates with me in a HCI and security context, as long after a project becomes a product and all parties have moved on, people are left with the resulting solution for years – for better or for worse. I experienced a poignant moment in this sense at a demo in 2008 at the Royal Society Summer Science exhibition in London. The subject of the demo was a visual authentication system we called BDAS (Dunphy and Yan, 2007) where the user draws a password. The exhibit received a visit from one man who introduced himself as being nearly blind, and asked in a genuine tone, 'so what am I supposed to do with this?'. Security in particular is often focused on the average user. However, HCI research is more open to such specific design; security could learn more from this trend.

REFERENCES

De Angeli, A., Coventry, L., and Johnson, G. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human–Computer Studies*, **63**(1–2), 128–152.

Dirik, A.E., Memon, N., and Birget, J.-C. (2007). Modelling user choice in the PassPoints graphical password scheme. In *Proceedings of the 3rd symposium on Usable privacy and security*, 20–28.

Dunphy, P., Nicholson, J., and Olivier, P. (2008). Securing passfaces for description. In *Proceedings of the 4th Symposium on Usable Privacy and Security* (SOUPS '08), 24–35. New York: ACM.

Dunphy, P. and Yan, J. (2007). Do background images improve "draw a secret" graphical passwords? In *Proceedings of the 14th ACM conference on Computer and Communications Security* (CCS '07), 36–47. New York: ACM.

Dunphy, P., Fitch, A., and Olivier, P. (2008b). Gaze Contingent Graphical Passwords at the ATM. In *Proceedings of The 4th COGAIN Annual Conference on Communication by Gaze Interaction*, COGAIN '08, Prague, Czech Republic, September 2–3, 2008.

Suo, X., Zhu, Y. and Owen, G.S. (2005). Graphical Passwords: A Survey. In *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC '05), 463-472. Washington, DC: IEEE Computer Society.

Winograd, E., Smith, A. and Simon, E. (1982). Aging and the Picture Superiority Effect in Recall. *Journal of Gerontology*, 37(1), 70–75.

A note from the Editor

Firstly I would like to thank Stephen Hassard for his support to *Interfaces* as he steps down from his role as My PhD editor. I would like to welcome Shaun Lawson as his replacement. Little did Shaun realise as he sat in a Icelandic bar at Nordichi, not believing a beer could really cost that much, the hidden cost of a chat that would lead him to volunteer for this role.

Shaun Lawson is Professor of Social Computing in the School of Computer Science where he directs the Lincoln Social Computing (LiSC) Research Centre. His research is focused on social aspects of human–computer interaction. This includes investigations of how people engage with mobile and social platforms including online social networks (OSNs), micro-blogging services, and social and pervasive games. Much of his recent work is built upon the hypothesis that such technology provides a platform to deliver

interactive services which can be used for serious purposes and behaviour change. For instance he currently holds EU, HEFCE and EPSRC funding to, respectively, investigate how social computing can be used to: teach leadership skills, reduce energy consumption and improve engagement with psychological treatments for mental health disorders. Follow Shaun on Twitter at **twitter.com/shaunlawson**.

MY PHD

If you are a PhD student just itching to tell the world about your research or if you've enjoyed reading about some of the emerging areas of research that the My PhD column has recently discussed then we would like to hear from you.

We are currently accepting one to two page summaries from PhD students in the UK and across Europe with a focus on being open and accessible to everyone in the HCI community.

If you would like to submit or would just like more information please contact Professor Shaun Lawson using the contact information below.

Dr Shaun Lawson, Professor of Social Computing, Director, Lincoln Social Computing (LiSC) Research Centre, University of Lincoln, UK

http://lisc.lincoln.ac.uk/shaun
slawson@lincoln.ac.uk

TAKING STE²PS

Melanie Volkamer, Centre for Advanced Security Research, Darmstadt University, and **Lynne Coventry**, Psychology and Communication Technology Lab, Northumbria University, invite a diverse range of researchers to join them and the other founders in STE²PS

In October 2010, Northumbria University hosted a European Workshop on usable privacy and security. The aim of this session was to start to bring together researchers and practitioners in this area to identify how we could best work together to resolve the usable security and privacy conundrum.

Researchers from throughout Europe attended this workshop, including the authors contributing to this special edition. As a result of this first meeting, STE²PS was formed. This year we will host a number of workshops at conferences to promote the group. The first was hosted by Melanie Volkamer in Germany, and the next will be a workshop at the British HCI conference in July. Next year, hopefully, we will host our own conference and 2013 will see a joint European conference with SOUPS.

What is STE²PS?
STE²PS is a volunteer organisation with members from academia, government, and industry who have an interest in improving socio-technical experiences in privacy and security systems. Members are from various disciplines, including computer scientists, engineers, and psychology researchers and practitioners. Our main focus is in the European community, though this is not absolute.

Our mission
Our mission is to advocate a scientific and engineering approach to the design of technical systems for which there is interaction with people ('socio-technical systems'). We focus on systems that provide security or privacy protection, as well as other related areas such as trust and assurance. Our goals are to increase awareness, develop methods and tools, to support teaching and training, and to design solutions for building and evaluating socio-technical systems for security and privacy protection.

STE²PS
Science, Teaching and Engineering for Socio-Technical Experiences of Privacy and Security

Why?
The design of socio-technical systems for security and privacy protection is still in its infancy. As Ivan Fléchais and Shamal Faily point out in their article, the need for usable security has been recognised for centuries and our current approaches to the problem are not succeeding, even though we have seen increased effort focused on building solutions that are more usable, and it is now time for a more scientific and system-wide approach to be taken. Following on from SOUPS in the US, STE²PS is intended to bring together the currently disparate European community in this area.

How?
To achieve our mission and goals, we do the following:

- Host events such as workshops and conferences.
- Participate in related events by publishing and presenting.
- Host an online forum to share research reports, methods and education.

Your involvement
The success of this group will be dependent on participation from the diverse range of researchers in this area. If you would like to find out more and get on our mailing list then please contact us.

Contact: Lynne Coventry
lynne.coventry@northumbria.ac.uk

With special track: Commercialising Context

Fourteen years after the first CONTEXT conference in 1997 — and 60 years after Prior laid the foundation for the field —, the *Seventh International and Interdisciplinary Conference on Modeling and Using Context (CONTEXT'11)* sets out to extend foundational research on context and to evaluate the status and consequences of context research, as well as to address new questions for the field.

CONTEXT'11 will provide a forum for presenting and discussing high-quality research and applications on context. The conference will include paper, poster, and video presentations, system demonstrations, workshops, and a doctoral consortium. The conference invites researchers and practitioners to share insights and cutting-edge results from the wide range of disciplines concerned with context, including: Cognitive Sciences (Linguistics, Psychology, Philosophy, Computer Science, Neuroscience), Social Sciences and Organizational Sciences, and all application areas, including Medicine and Law. The motto of the CONTEXT'11 special track "Commercialising Context" was chosen to reflect both the fact that context research has found numerous successful applications in recent years and the fact that context itself has become a product that can be sold. Context-aware services can support their users unobtrusively and offer promising revenues. However, when context is no longer something private but processed and shared through the web, profound questions are raised about privacy and the general consequences of the technology.

Yet, the new context-aware services can also be a scientific tool for context-research itself. Context-aware services offer new ways for studying social context and its interaction with other types of context on a sociologically significant scale. For linguistic studies, context-aware mobile phones and chat programs, for instance, can be a tool for automatically obtaining context-annotated dialogues, with which the influence of context on meaning can be empirically assessed.

IMPORTANT DATES

May 8, 2011	Full papers, posters, videos, and demo abstracts
June 5, 2011	Notification of acceptance
June 19, 2011	Camera-ready papers

SUBMISSION

CONTEXT'11 will be an interdisciplinary forum. All submissions will be evaluated not only for their technical merit but also for their accessibility to an interdisciplinary audience. Works that transcend disciplinary boundaries are especially encouraged.

Full papers will be accepted for oral presentation or as poster. All accepted full paper submissions will be published in the proceedings which appear as a volume of Springer Lecture Notes in Artificial Intelligence. Accepted posters and demonstrations will be presented at the poster session. Videos will be presented as part of the conference program. The associated abstracts will be published in a brochure distributed to attendees.

See author instructions and format templates on the conference website for further details.

Program Chairs (context11-pch@teco.edu):

Hedda R. Schmidtke, KIT TecO, Germany
Anders Kofod-Petersen, NTNU, Norway
Kenny R. Coventry, Northumbria University, United Kingdom

General Chairs:

Michael Beigl, Karlsruhe Institute of Technology, Germany
Henning Christiansen, Roskilde University, Denmark
Thomas Roth-Berghofer, University of Hildesheim, Germany

Symposium On Usable Privacy and Security

SOUPS 2011

July 20–22, 2011, Pittsburgh, PA

The 7th Symposium on Usable Privacy and Security (SOUPS) brings together an interdisciplinary group of researchers and practitioners in human–computer interaction, security, and privacy. The programme features technical papers, posters, panels, invited talks and discussions. There will also be a number of workshops and tutorials. This year SOUPS will be held in Pittsburgh, PA, July 20–22, 2011.

Topics covered by this symposium include

- innovative security or privacy functionality and design
- new applications of existing models or technology
- field studies of security or privacy technology
- usability evaluations of new or existing security or privacy features
- security testing of new or existing usability features
- longitudinal studies of deployed security or privacy features
- the impact of organisational policy or procurement decisions
- lessons learned from the deployment and use of usable privacy and security features

The 8th International Symposium on Visualization for Cyber Security will be held in conjunction with SOUPS on July 20, 2011.

www.vizsec2011.org

cups.cs.cmu.edu/soups/2011

EXECUTIVE COMMITTEE 2010–2011

Tom McEwan UK Chair
David England Membership Secretary
Corina Sas Treasurer
John Knight Communications Chair
George Buchanan Research Chair
Janet Read Education Chair
Jakub Dostal Student Representative Chair
Aaron Quigley Scottish Chair

CHAIR'S ADVISORS

Russell Beale HCI2012 co-Chair
Adrian Williamson BCS Liaison

SOUTH ENGLAND

John Knight Communications Chair
Nick Bryan-Kinns PR & Marketing, UsabilityNews Advisor
George Buchanan Research Chair
Andy Smith India/China Liaison
Dianne Murray Editor, *Interacting with Computers*
Jennefer Hart, **Shaun Lawson**, **Shailey Minocha** *Interfaces* Contributing Editors
Jonathan Earthy HCI Accreditation Scheme
Tony Russell-Rose Committee Member

NORTH ENGLAND

Corina Sas Treasurer
Janet Read Education Chair
David England Membership Secretary
Andy Dearden IFIP Liaison
Alan Dix, **Barbara McManus** Éminences Grises

WALES & SW ENGLAND

Russell Beale HCI2012 co-Chair
Ben Cowan HCI2012 co-Chair and JISC Mailing List
Daniel Cunliffe Regional Liaison
Matt Jones Regional Liaison
Steven Welti Student Representative

SCOTLAND & NE ENGLAND

Tom McEwan UK Chair
Lynne Coventry Interfaces Magazine Editor and HCI2011 Chair
Linda Little HCI2011 Chair
Jakub Dostal Student Representative Chair
Aaron Quigley Scottish Chair
Ingi Helgason Create2010 Chair
Emilia Sobolewska Communications Support

VACANT ROLES

Offers of help always welcome
Webmaster/Web Developers
Student Representatives
Industry & Public Sector Representatives
Interfaces Magazine contributors
UsabilityNews contributors

BCS CONTACT

E groups@hq.bcs.org.uk
T +44 (0)1793 417 478

BCS, The Chartered Institute for IT
First Floor, Block D, North Star House,
North Star Avenue, Swindon, UK, SN2 1FA
T +44 (0)1793 417 417
F +44 (0)1793 480 270
www.bcs.org

BCS Interaction Group is served by regionally based sub-groups with representatives from a broad range of academic and industrial centres of HCI interest. The sub-groups meet informally every few weeks to progress work, and all participants are committed to promoting the education and practice of HCI and to supporting HCI people in industry and academia. For contact details of the people in each sub-group, please select from the following:

INTERACTION COMMITTEE MEMBERS

Jacqueline Archibald University of Abertay Dundee **e** J.Archibald@abertay.ac.uk
Russell Beale University of Birmingham **t** 0121 414 3729 **f** 0121 414 4281 **e** R.Beale@cs.bham.ac.uk
Nick Bryan-Kinns Queen Mary University **t** 020 7882 7845 **e** nickbk@dcs.qmul.ac.uk
George Buchanan City University London **t** 0207 040 8469 **e** george.buchanan.1@city.ac.uk
Ben Cowan University of Birmingham **t** 0121 414 4787 **e** B.R.Cowan@cs.bham.ac.uk
Lynne Coventry Northumbria University **e** lynne.coventry@northumbria.ac.uk
Daniel Cunliffe University of Glamorgan **t** 01443 483694 **f** 01443 482715 **e** djcunlif@glam.ac.uk
Andy M Dearden Sheffield Hallam University **e** A.M.Dearden@shu.ac.uk
Alan Dix Lancaster University **t** 07887 743446 **f** 01524 510492 **e** alan@hcibook.com
Jakub Dostal The University of St Andrews **t** 01334 463260 **e** jd@cs.st-andrews.ac.uk
Jonathan Earthy Lloyd's Register **t** 020 7423 1422 **f** 020 7423 2304 **e** jonathan.earthy@lr.org
David England Liverpool John Moores University **t** 0151 231 2271 **f** 0151 207 4594 **e** d.england@livjm.ac.uk
Phil Gray University of Glasgow **e** pdg@dcs.gla.ac.uk
Jennefer Hart The Open University **t** 01908 652817 **e** jennefer.hart@open.ac.uk
Ingi Helgason Edinburgh Napier University **t** 0131 455 2750 **e** i.helgason@napier.ac.uk
Matt Jones Swansea University **e** matt.jones@swansea.ac.uk
John Knight **e** John.Knight@intiuo.com
Shaun Lawson University of Lincoln **e** s.lawson@lincoln.ac.uk
Linda Little Northumbria University **e** l.little@northumbria.ac.uk
Tom McEwan Edinburgh Napier University **t** 0131 455 2793 **f** 0131 455 2727 **e** t.mcewan@napier.ac.uk
Barbara McManus University of Central Lancashire **t** 01772 893288 **f** 01772 892913 **e** bmcmanus@uclan.ac.uk
Shailey Minocha The Open University **e** s.minocha@open.ac.uk
Dianne Murray **t** 0208 943 3784 **f** 0208 943 3377 **e** dianne@soi.city.ac.uk
Aaron Quigley University of St Andrews **t** 01334 461623 **e** aquigley@cs.st-andrews.ac.uk
Janet Read University of Central Lancashire **t** 01772 893285 **e** jcread@uclan.ac.uk
Tony Russell-Rose EMEA **t** 0203 166 4444 **e** trose@endeca.com
Corina Sas Lancaster University **e** corina@comp.lancs.ac.uk
Emilia Sobolewska Edinburgh Napier University **t** 0131 455 2700 **e** e.sobolewska@napier.ac.uk
Andy Smith Thames Valley University **t** 01753 697565 **f** 01753 697750 **e** andy.smith@tvu.ac.uk
Steven Welti Swansea University
Adrian Williamson zonal **t** 01506 485770

INTERFACES MAGAZINE

Lynne Coventry Editor
Shaun Lawson My PhD Editor
Jennefer Hart Profile Editor
Shailey Minocha Reviews Editor
Fiona Dix Production Editor

EDITOR INTERACTING WITH COMPUTERS

Dianne Murray

RELEVANT URLS

British HCI Group: **www.bcs-hci.org.uk**
UsabilityNews: **www.usabilitynews.com**
IWC: search for Interacting with Computers
HCI2010: **www.hci2010.org**
HCI2011: **www.hci2011.co.uk**

Interfaces is published quarterly by BCS Interaction (a Specialist Group of the British Computer Society) and is available in print and as download. Interfaces is produced on a not-for-profit basis by volunteers for the good of the international HCI community.

Interfaces editorial policy is focused on promoting HCI and its community in all facets, representing its diversity and exemplifying its professional values by promoting knowledge, understanding and awareness to the benefit of all and harm to none. Editorial decisions are based on promoting these core values with the Editor being accountable to BCS Interaction Specialist Group and BCS for the content of the magazine. As such the Editor has the right to refuse publication with recourse to BCS Interaction Specialist Group and BCS in cases of arbitration.

The views and opinions expressed in Interfaces are strictly those of the relevant authors attributed to articles and do not necessarily represent those of BCS Interaction Specialist Group, British Computer Society or any associated organisation. Interfaces does not accept responsibility for the views expressed by contributors and unless explicitly stated (where authors are publishing at the behest of an organisation or group), authors are acting in a personal capacity and expressing personal opinions that may or may not represent the views and opinions of any organisation, employer, person or group attributable to them.

 ISSN 1351-119X.