Multi-Disciplinary Aspects of Cyber Security

M. Angela Sasse
University College London, UK

Research Institute for Science of Cyber Security
www.ucl.ac.uk/cybersecurity/

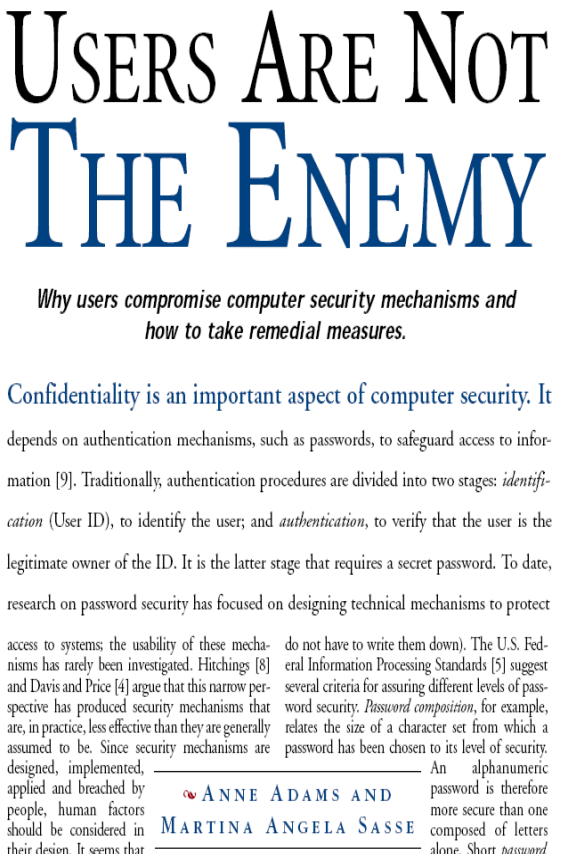
Academic Centre of Excellence for Cyber Security Research
http://sec.cs.ucl.ac.uk/ace_csr/

Overview

1. Why does cyber security need a multi-disciplinary approach?
2. Which research disciplines can contribute?
3. My own experience (in usable security and economics), and other notable examples of multi-disciplinary cyber security research
4. Challenges for multi-disciplinary cyber security research
5. Meeting those challenges through an outcome-oriented, evidence-based approach

My own multi-disciplinary journey

- 1996: Usability study to explain password security (with Anne Adams)
- Published in 1999: “Users Are Not the Enemy”
- Also 1999: Whitten & Tygar *“Why Johnny can’t encrypt”*
- Started research in usable security



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

ANNE ADAMS AND MARTINA ANGELA SASSE

Adams & Sasse CACM 1999

What has been achieved over the past 10+ years?

- 2005: Symposium on Usable Security and Privacy (SOUPS)
- 2005 Cranor & Garfinkel book
- 2008: Security & Human Behaviour (SHB)
- 2009: US National Academy of Sciences Workshop on *Usable Security and Privacy*
- Papers in CHI, CCS, Usenix, NSPW
- Taught modules in usable security

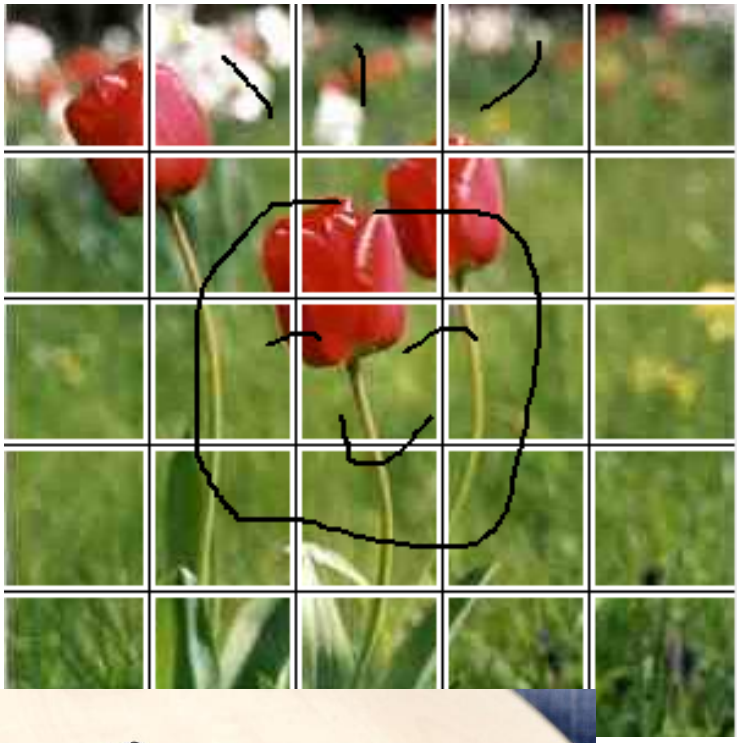
Has it made a difference in practice?

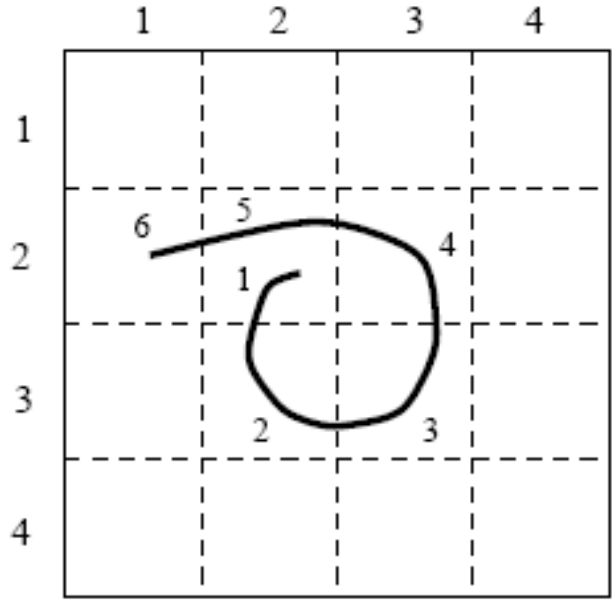
- Consider authentication:
  - Nielsen (2000) said that biometrics are highly usable and would replace passwords.
  - Schneier (2000) and Gates (2004) predicted that passwords would become obsolete.
- Instead:
  - People have more passwords. Longer ones.
  - They write down, store, re-use and re-cycle passwords.
  - They have to think up and recall back-up credentials for passwords. And solve a CAPTCHA before they are allowed to attempt to remember them.

Usable security research: the quest for the password replacement

- Example Passfaces. Memorable, yes. But:
  - Too slow for regular authentication (Brostoff & Sasse, HCI 2000)
  - Selection biases result in low guessing difficulty (Jermyn et al., USENIX Security1999)
  - With more than one Passfaces password, users get confused (Everitt et al., CHI 2009)

Draw-a-Secret & BDAS

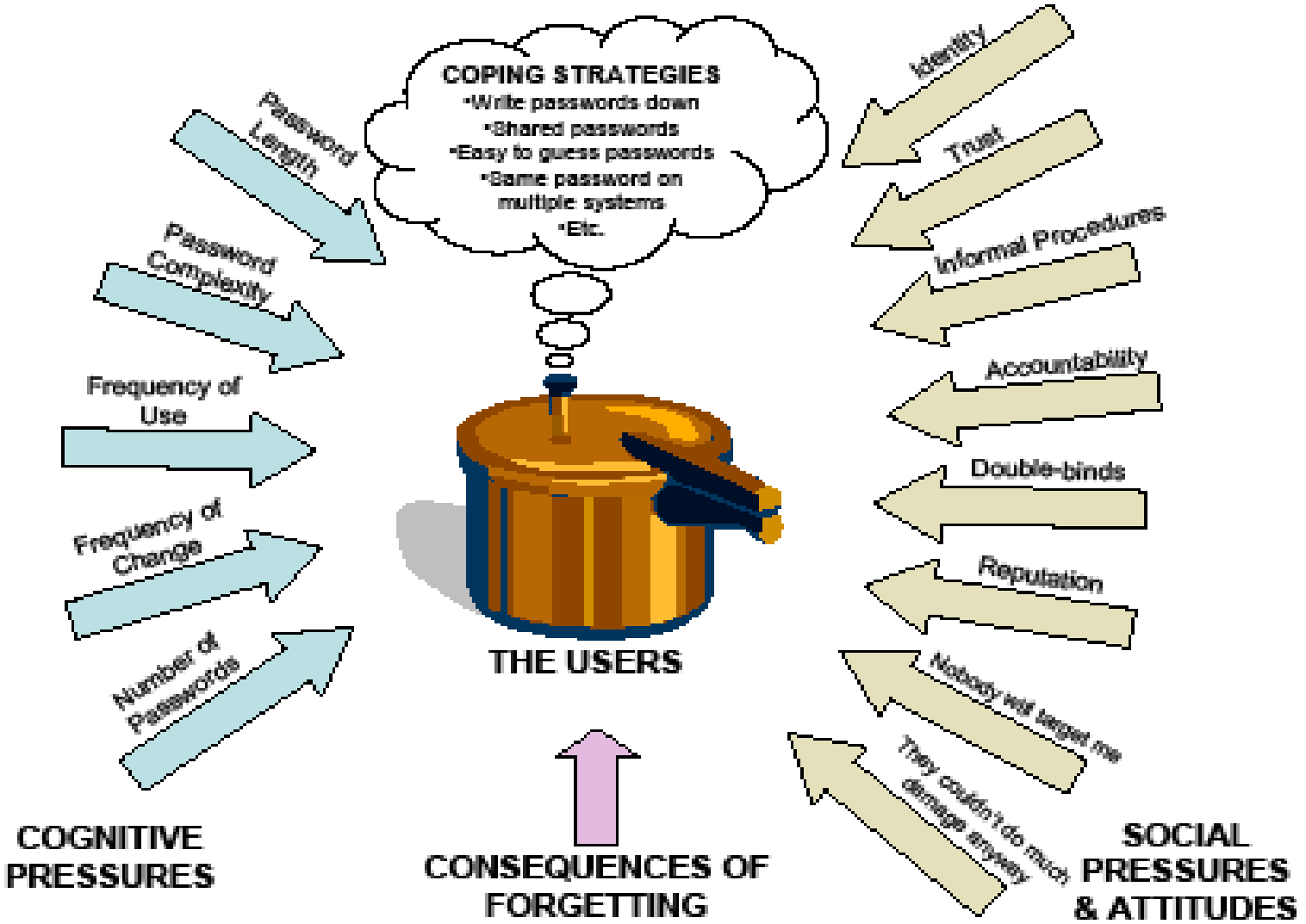




Yan et. al

More examples of ‘usable authentication’

- Via Rorschach inkblot tests
- By singing your password to the computer
- By thinking your password (free EEG thrown in)
- Schneier: fMRI would be cool
- Making users watch ads, and hitting 4 frames
- Ringing up your friends in the middle of the night, asking them to find the credential you have them months ago, and log into a system to confirm it’s you



Allendoerfer & Pai (2005): Human Factors Considerations for Passwords and Other User Identification Techniques. US DOT/FAA/CT- 05/20

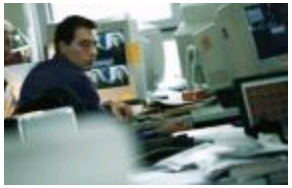
Foundations of usability

1. Fitting the system around the human – not bending the human to fit the task
2. For users, security is a secondary task – accept that they want as little workload and disruption as possible
3. More complex than 'what's easy to remember' - *'It Depends':*
   - on specific user characteristics (universal access), *frequency of use*, *interference*
   - physical and social context of use
   - characteristics of the device (Sasse et al., 2001)

has general & specific characteristics

USER

interacts with



SYSTEM/ SERVICE

to attain

GOAL

"get ticket for Justin Bieber concert"

interaction takes place in a

CONTEXT

physical

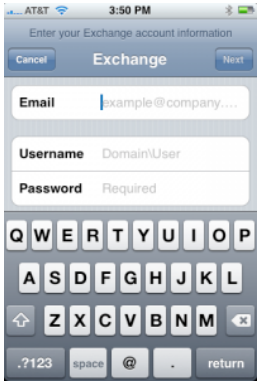
social

cultural

temporal

using a specific

DEVICE



Really usable authentication

- Authenticate users when needed – but minimize the effort it requires from them
  - Move from explicit to implicit authentication – let technology do the work
  - Learning from e-commerce: recognize users through cookies, history/patterns, etc.
  - Using tokens or biometrics
  - Exploit modality of interaction – touch on touchscreens, video, audio
- Maximize the benefits for users and/or organizations – “productive security”

Security that supports user goals

Give an Allowance with Amazon PayPhrase

What is Amazon PayPhrase?

PayPhrase is an easy-to-remember shortcut to the payment and shipping information in your Amazon.com account. Each PayPhrase can be configured with simple controls, including monthly spending limits and e-mail alerts, so you can share your account with family members without sharing your credit card number or account password.

PayPhrase allowance controls include:

- Monthly spending limits
- Unspent allowance roll-over settings
- Order approval by e-mail or text message

› Create your PayPhrase

Re-design burdensome security

- ‘A tale of two laptops’
- Re-authenticating every 15 mins because of screenlocks when you haven’t moved
- Having to create 4 passwords p.a. for systems accessed 1-2 p.a.

Obstacle security = unproductive security

“CAPTCHAs waste 17 years of human effort every day” (Pogue 2012)

There is no “usable CAPTCHA” –must look for ways of distinguishing humans from bots without bothering humans

Security people used to know usability

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
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;**
4. The system ought to be compatible with telegraph communication;
5. **The system must be portable, and its use must not require more than one person;**
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.**

Auguste Kerckhoffs, 'La cryptographie militaire',
Journal des sciences militaires, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.

Problem: today, security people don't track long-term impact of their decisions

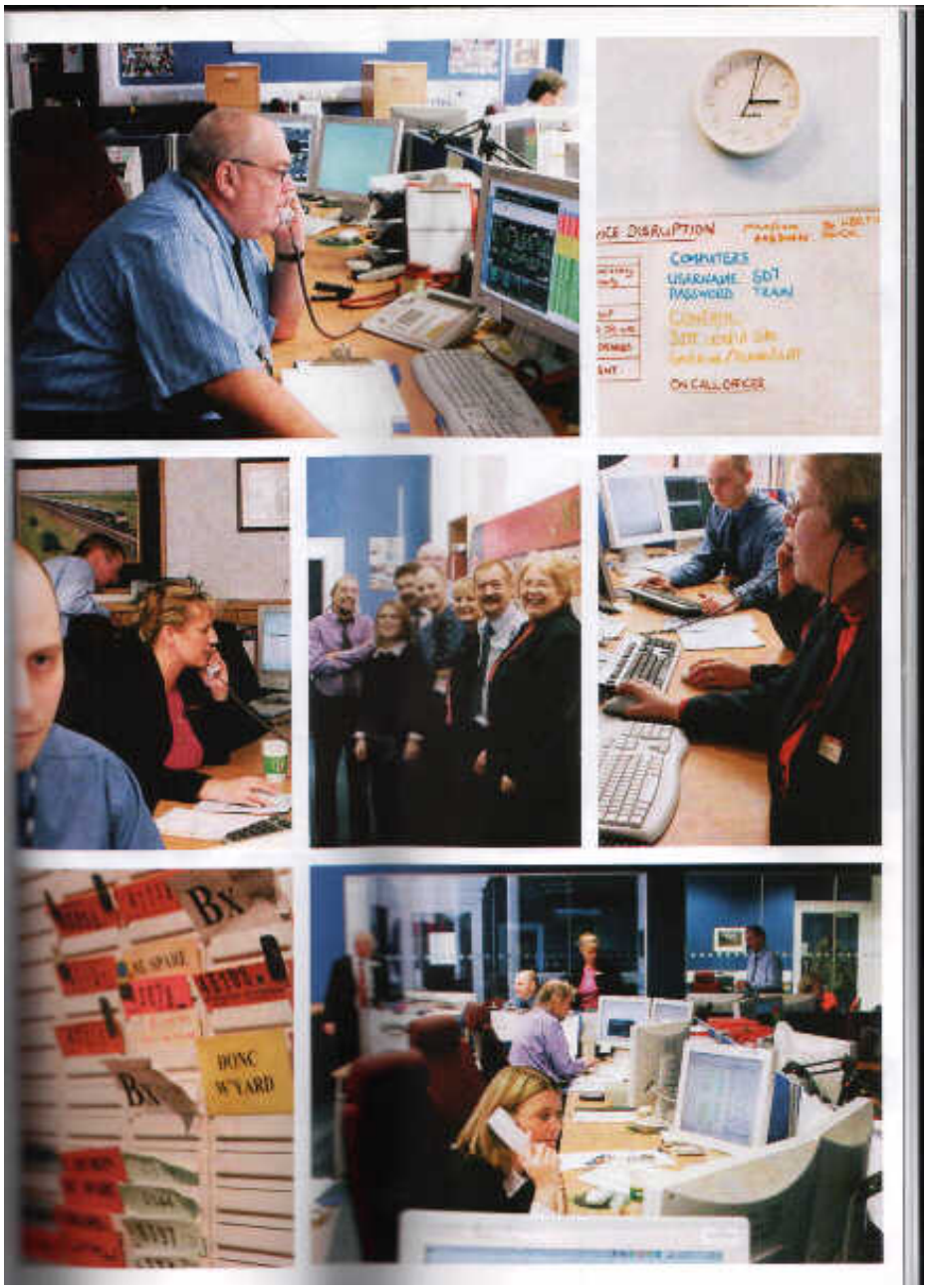
Such as - employees

- not using corporate laptops
- stop logging in from home
- not collaborating with externals
- leaving the organization

… and the

- vulnerabilities created by workarounds (e.g password sharing, mouse jigglers)
- bad general security perceptions and habits

- Glossy brochure of UK railway company … complete with passwords on whiteboard



Lack of evidence, and of reflective practice

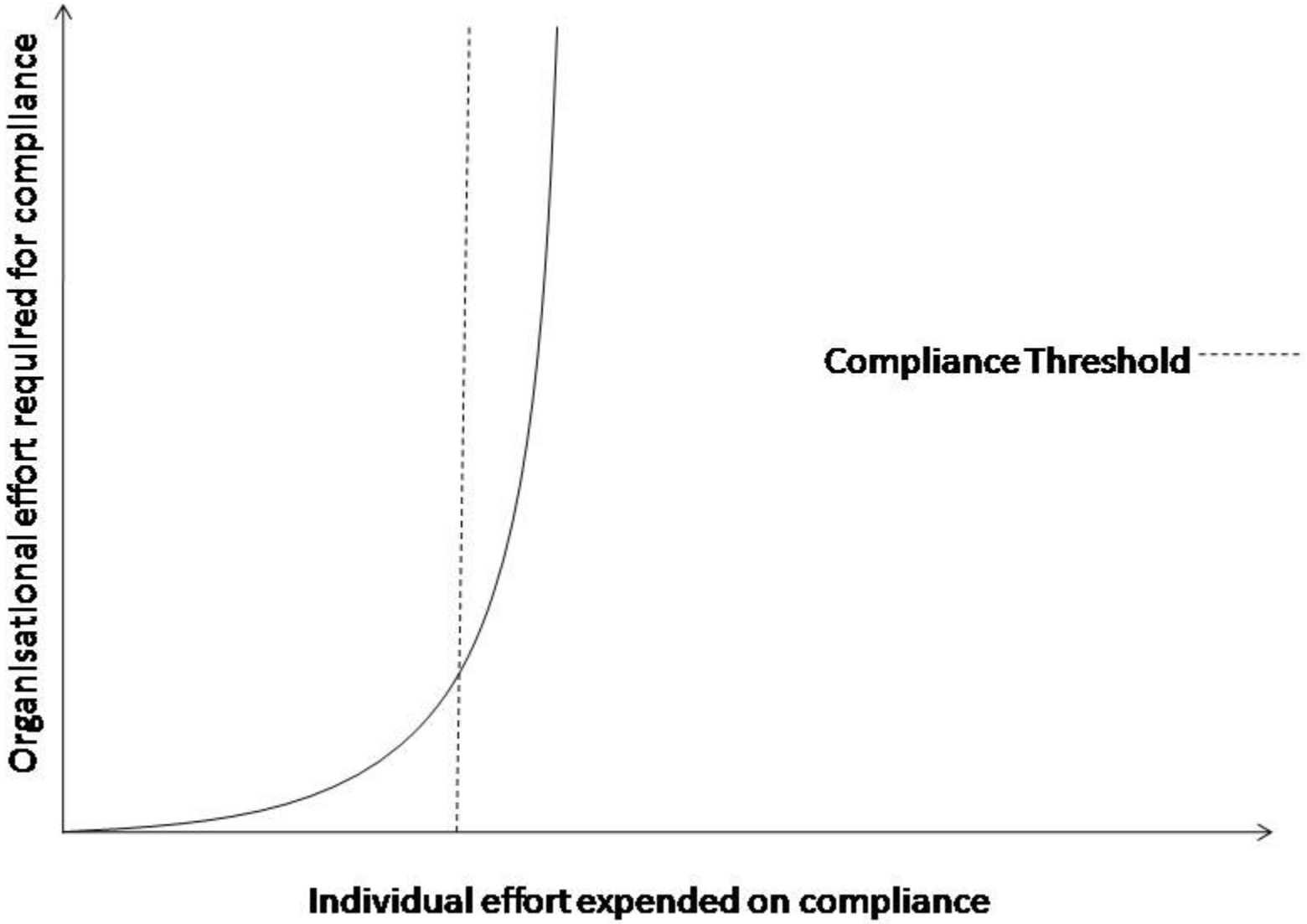
- security profession is a craft
- dominated by ‘Best Practice’
- impact of security measures rarely evaluated – at least not in a meaningful way
- researchers need to challenge this without putting practitioners onto defensive
- move to an evidence-based approach …

Economics to the rescue

- Workshop on Economics of Security (WEIS), founded by Ross and Anderson and Bruce Schneier, is now 10 years old
- *"Security people value users' time at zero."* (Herley NSPW 2009)
- Risk consumers face is simply not worth the effort (externalities) that most security measures create for them – *"rational rejection of security advice"*.

The ‘Compliance Budget’

Beautement et al. 2008

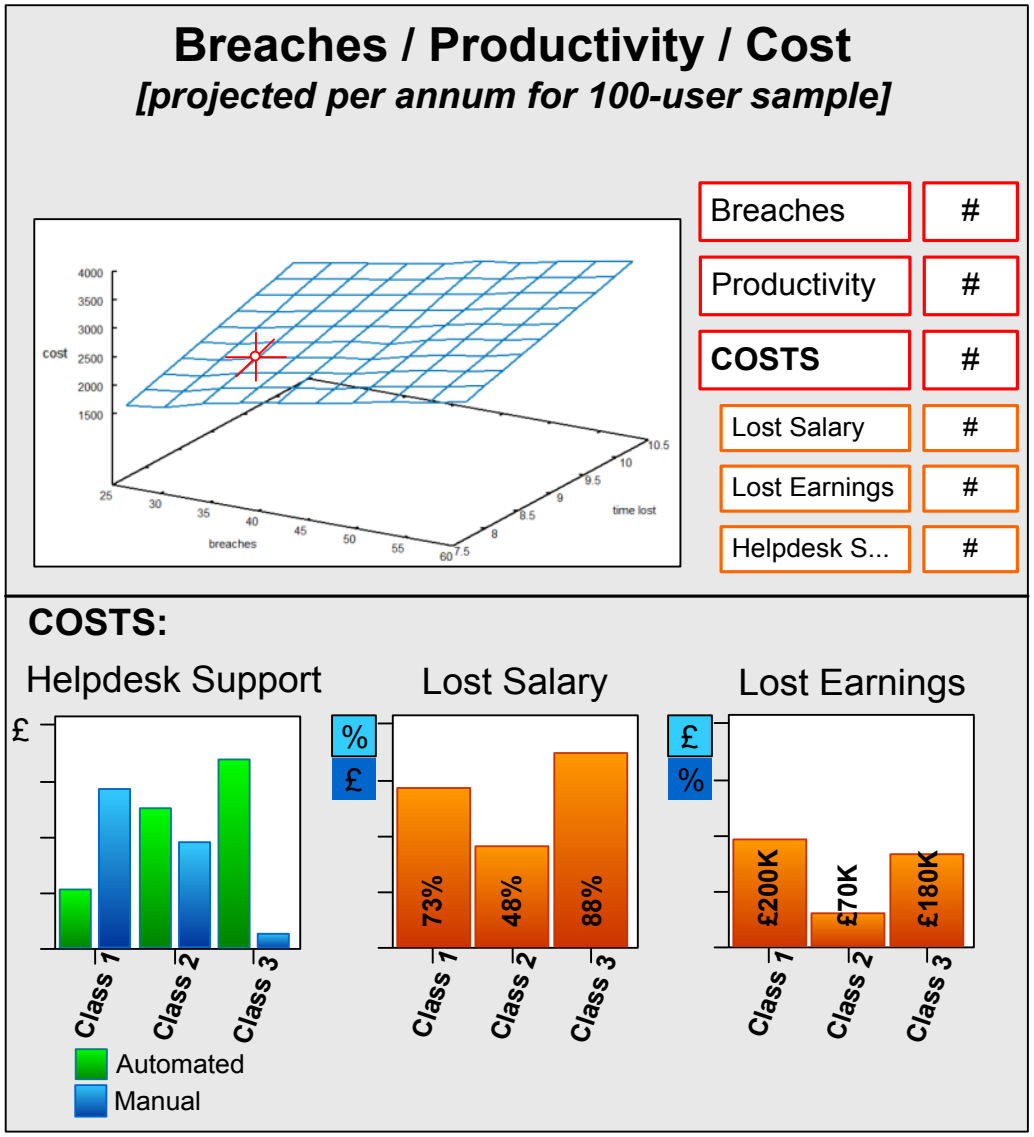


Add *Cognitive Science* to understand security decision-makers

- Shiu et al. 2011 studied security professionals' decision-making on security policies and investments
- without economic framing, security professionals focus on security
- security professionals need to see impact of their decision in context of risk, cost, productivity to make better decisions

Example dashboard interface for CISOs

Parkin et al. 2010



Cost of security measures

Pallas 2008

Meta-Measure	Initial Costs (once)	Enforce-ment Costs	Loss from non-compliance
Architect. Means	high	none / negligible	none / negligible
Formal Rules	low	high	high
Informal Rules	medium	low (spont.)	high

Security by Design – Crime Science

- A scientific approach for the prevention of crime
- Understanding
  - short-term motives of attackers (rational actor similar to economics)
  - routine activities
  - patterns of attacks
- Focused on removing opportunities for attackers – e.g. vulnerabilities in cyber security

Crime Science is multi-disciplinary

- *"makes use, amongst others, of knowledge and methods of Geography, Urban Development, Mathematics, Industrial Design, Construction Engineering, Medical Science, Economics, Computer Science, Psychology, Sociology, Criminology, Law, and Public Management"*
- **Empirical** investigation of crimes to gain understanding of factors and mechanics
- **Evidence-based** evaluations of interventions

Example application in cyber security

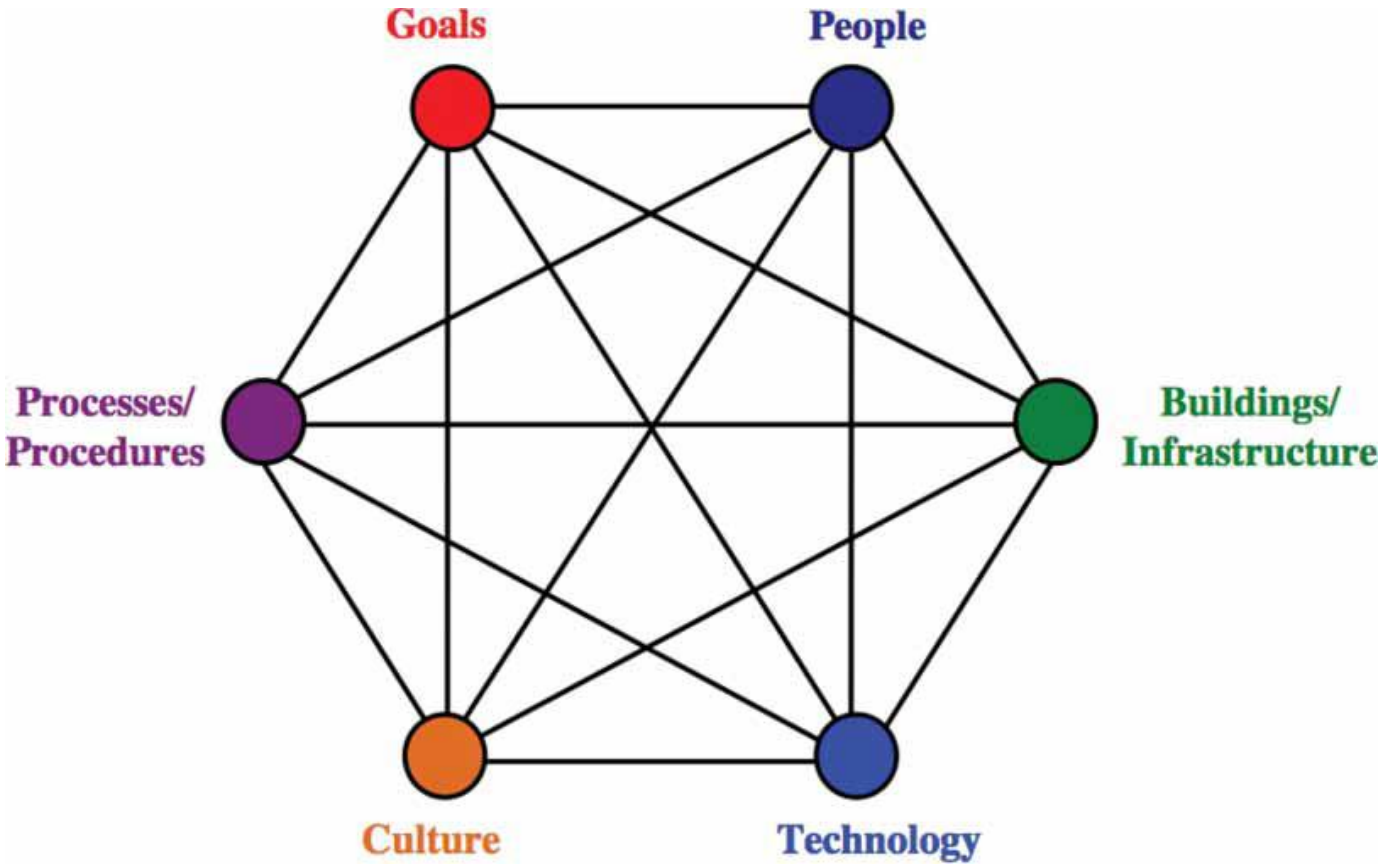
- Stajano & Wilson (2011) systematic analysis of principles used by fraudsters
  1. Distraction
  2. Social Compliance
  3. Herd behaviour
  4. Dishonesty
  5. Deception
  6. Need and Greed
  7. Time
- and how this can be applied to system design

Why is application to cyber security relevant?

"… even well intended security policies or mechanisms are ignored or simply too costly to implement. The classical example is the user who is forced to choose a strong password that he cannot remember. As a consequence the user writes the password on a yellow sticky and attaches it to his screen. Another example is given by Herley who estimates that the cost of Phishing is probably dwarfed by the burden on the users who are asked to comply with a variety of advice designed to stop phishing. To make Information Security more effective, economic and human factors must be taken into account."

Haertel et al. (2010)

Socio-technical framework



… into which different factors can be integrated
Challenger & Clegg (2011)

Converging insights from different disciplines

1. Stakeholders act rationally, most of the time – behavior is driven by perceived cost and benefits of their actions
2. Rational does not equal perfect: incomplete knowledge, biases in reasoning, and short-termism lead to non-optimal decisions
3. Once established, habits are powerful
4. Security measures which place cost on any stakeholder without proportionate benefit will fail
5. Stakeholders need incentives to invest in detailed risk analysis, security-by-design, evaluation of effectiveness

Challenges of multi-disciplinary research

1. Substantive
   - application of knowledge from a different discipline cannot be ‘smash & grab’
   - collaboration helps, but requires development of common vocabulary and set of goals
2. Methodological
   - agreeing on reseach designs and methods (data types, data collection methods)
3. Hard to publish multi-disciplinary security research in top venues

Over-coming the challenges

1. Outcome-oriented perspective can provide common focus for different disciplines
2. Empirical (evidence-based) evaluation of outcomes helps to build cumulative knowledge base for new multi-disciplinary science of cyber security
3. Conducting research in real-world context has benefits for researchers and practitioners
4. Methodological differences can be overcome by common commitment to good science
5. Open-minded approach – insights from multi-disciplinary research can advance science in home disciplines

Example of methodology

- Caputo et al. 2012 – study on effectiveness of training against phishing, in organization, not just 1-shot intervention
- Clearly stated scientific method
  - Controlled sampling
  - Realistic situations
  - Scientific and documented processes
  - Clearly stated hypotheses
  - Data, tools and techniques made available for others to use
  - Data analysis to support evidence-based cyber security decisions

Conclusions

1. Long list of disciplines that could contribute to cyber security
   - human factors, psychology, cognitive science, behavioral economics and crime science are emerging as fruitful collaborations
   - anthropology, archaeology, biology, design science, history … (SHB provides good example of variety)
2. Outcome-oriented, evidence-based, quality research provides focus and chance to connect to connect to practitioners, and advance practice
3. Requires investment in collaborations, willingness to learn, and take risks

Comforting words – from a physicist

"A scientist is supposed to have a complete and thorough knowledge, at first hand, of some subjects and, therefore, is usually expected not to write on any topic of which he is not a master. This is regarded as a matter of noblesse oblige. For the present purpose I beg to renounce the noblesse, if any, and to be the freed of the ensuing obligation. My excuse is as follows: We have inherited from our forefathers the keen longing for unified, all-embracing knowledge. The very name given to the highest institutions of learning reminds us, that from antiquity to and throughout many centuries the universal aspect has been the only one to be given full credit.

But the spread, both in and width and depth, of the multifarious branches of knowledge by during the last hundred odd years has confronted us with a queer dilemma. We feel clearly that we are only now beginning to acquire reliable material for welding together the sum total of all that is known into a whole; but, on the other hand, it has become next to impossible for a single mind fully to command more than a small specialized portion of it. I can see no other escape from this dilemma (lest our true aim be lost for ever) than that some of us should venture to embark on a synthesis of facts and theories, albeit with second-hand and incomplete knowledge of some of them - and at the risk of making fools of ourselves."

Erwin Schrödinger, "What is Life?" (1944)

References

- A. Adams & M. A. Sasse (1999): Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures. *Communications of the ACM,* 42 (12), pp. 40-46 December 1999.
- S. Arnell, A. Beautement, P. Inglesant, B. Monahan, D. Pym & M. A. Sasse (2012) Systematic Decision Making in Security Management - Modelling Password Usage and Support. *International Workshop on Quantitative Aspects in Security Assurance* (QASA 2012). Pisa, Italy.
- A. Beautement, M. A. Sasse & M. Wonham, M. (2008): The compliance budget: Managing security behaviour in organisations. *Procs NSPW 2008*, 47-58.
- S. Brostoff & M. A. Sasse (2000): Are Passfaces more usable than passwords? A field trial investigation. *Procs HCI 2000.* Sunderland, UK, pp. 405-424. Springer.
- D. D. Caputo, S. Lawrence Pfleeger, J. D. Freeman & M. Eric Johnson(2012): Going Spear Phishing: Exploring Embedded Training and Awareness. http://www.mitre.org/work/tech_papers/2012/12_4238/
- A.Campbell (2007): Usability myths and professionals. http://alastairc.ac/2007/09/usability-myths-and-professionals/
- R. Challenger & C. W. Clegg (2011): Crowd disasters: A socio-technical systems perspective. *Contemporary Social Science, Special Issue: Crowds in the 21st Century*, 6, 343-360.
- L.F. Granor & S. Garfinkel (2005): Usable Security -Designing Secure Systems that People Can Use. O'Reilly.
- K. M. Everitt, T. Bragin, J. Fogarty, & T. Kohno (2009): A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords. *Proceedings of CHI 2009.* pp. 889-898.
- P. H. Hartel, M. Junger, M. & R.J. Wieringa (2010) *Cyber-crime Science = Crime Science + Information Security.* Technical Report TR-CTIT-10-34, Centre for Telematics and Information Technology University of Twente, Enschede. ISSN 1381-3625

- C. Herley (2009): So Long, And No Thanks For The Externalities: the rational rejection of security advice by users. *Procs NSPW 2009*, Oxford, UK.
- P. G. Inglesant & M. A. Sasse (2010). The True Cost of Unusable Password Policies: password use in the wild. *Procs CHI 2010*. Atlanta, Georgia, 383-392.
- I. Jermyn, A. Mayer, F. Monrose, A. Rubin & M. K. Reiter (1999): The design and analysis of graphical passwords. *Procs USENIX Security Symposium*, 1-14.
- F. Pallas (2009): Information Security Inside Organizations: A Positive Model and Some Normative Arguments Based on New Institutional Economics. PhD Thesis,Technische Universität Berlin, Germany.
- S. Parkin, A. van Moorsel, P. G. Inglesant & Sasse, M.A. (2010) A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions. NSPW 2010: *Procs NSPW 2010,* 33-49.
- D. Pogue (2012): Time to kill off CAPCHAs. *Scientific American,* March 2012,
- M. A. Sasse, S. Brostoff, & D. Weirich (2001): Transforming the “Weakest Link": a human-computer interaction approach to usable and effective security. *BT Technology Journal*, Vol 19 (3) July 2001, 122-131.
- S. Shiu, A. Baldwin, Y.Beres, M. Cassa Mont, G. Duggan, H. Johnson & C. Middup (2011): Economic methods and decision making by security professionals. Procs WEIS 2011.
- E. Schrodinger (1944): What is life? The Physical Aspect of the Living Cell. *whatis**life**.stanford.edu/LoCo_files/What-is-**Life**.pdf*
- *F. Stajano & P. Wilson (2011): Understanding scam victims: seven principles for systems security. Communications of the ACM* March 2011, 70-75