Designing for the Human Element in Security

M. Angela Sasse

Professor of Human-Centred Technology,

Head of Information Security Research

Department of Computer Science

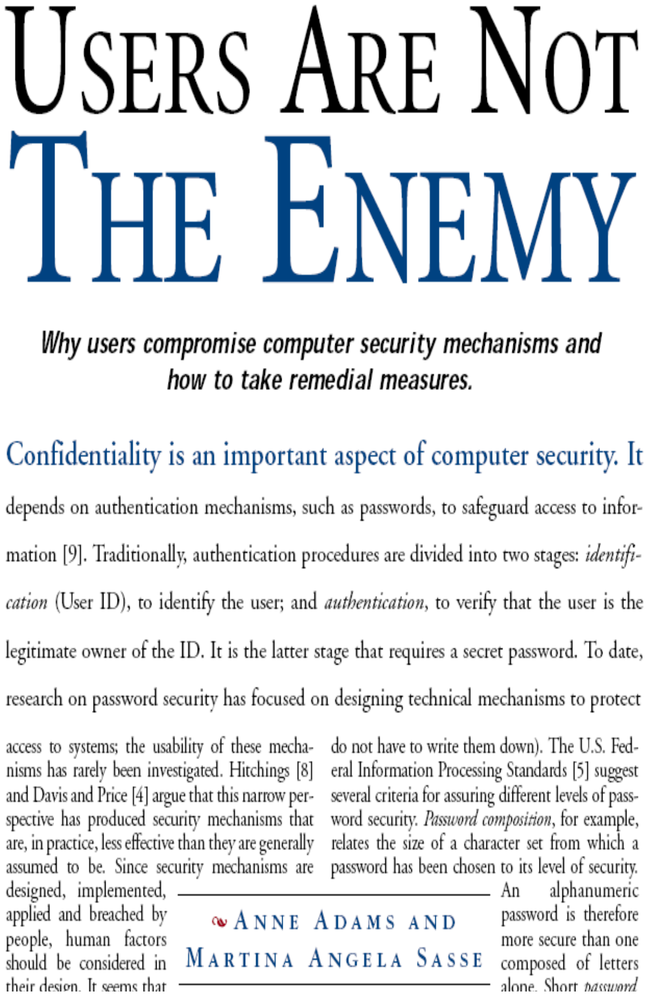
University College London, UK

a.sasse@cs.ucl.ac.uk

www.ucl.cs.ac.uk/staff/A.Sasse

History

- Study on escalating cost of password resets at BT: staff
  - Couldn't cope with workload generated by policies
  - circumvent security
  - don't understand threats and risks
- Also 1999: Whitten & Tygar *"Why Johnny can't encrypt"*



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

Anne Adams and Martina Angela Sasse

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*

Adams & Sasse CACM 1999

What Has Happened Over The Past Decade?

- Lots:
  - ACM SOUPS (Symposium on Usable Security and Privacy) since 2004
  - SHB (Security & Human Behaviour) since 2008
  - Papers in CHI, CCS, Usenix, NSPW …
  - Books: Cranor & Garfinkel, Shostack, Lacey
  - University modules usable security
  - White Paper on *Human Vulnerabilities in Security Systems (UK)* 2007
  - US National Academy of Sciences Workshop on *Usable Security and Privacy* 2009

And - has it made security (more) usable?

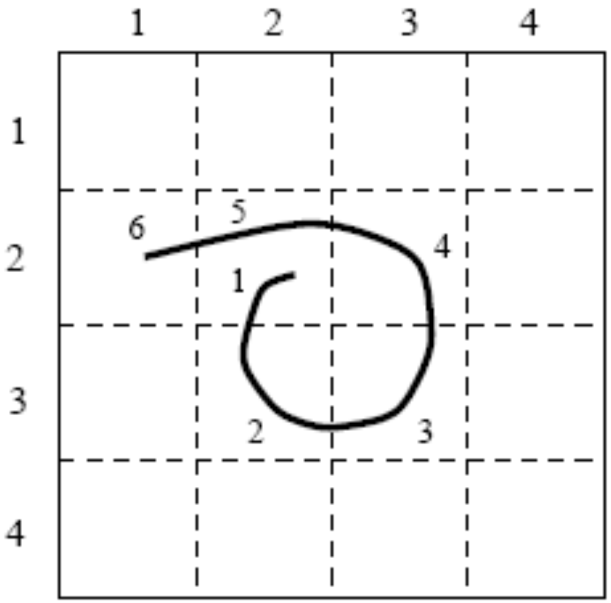
- Nielsen (2000) said that biometrics are highly usable and would replace passwords – hasn’t happened.
- Schneier (2000) and Gates (2004) predicted that passwords would become obsolete

- Didn’t happen. Why?

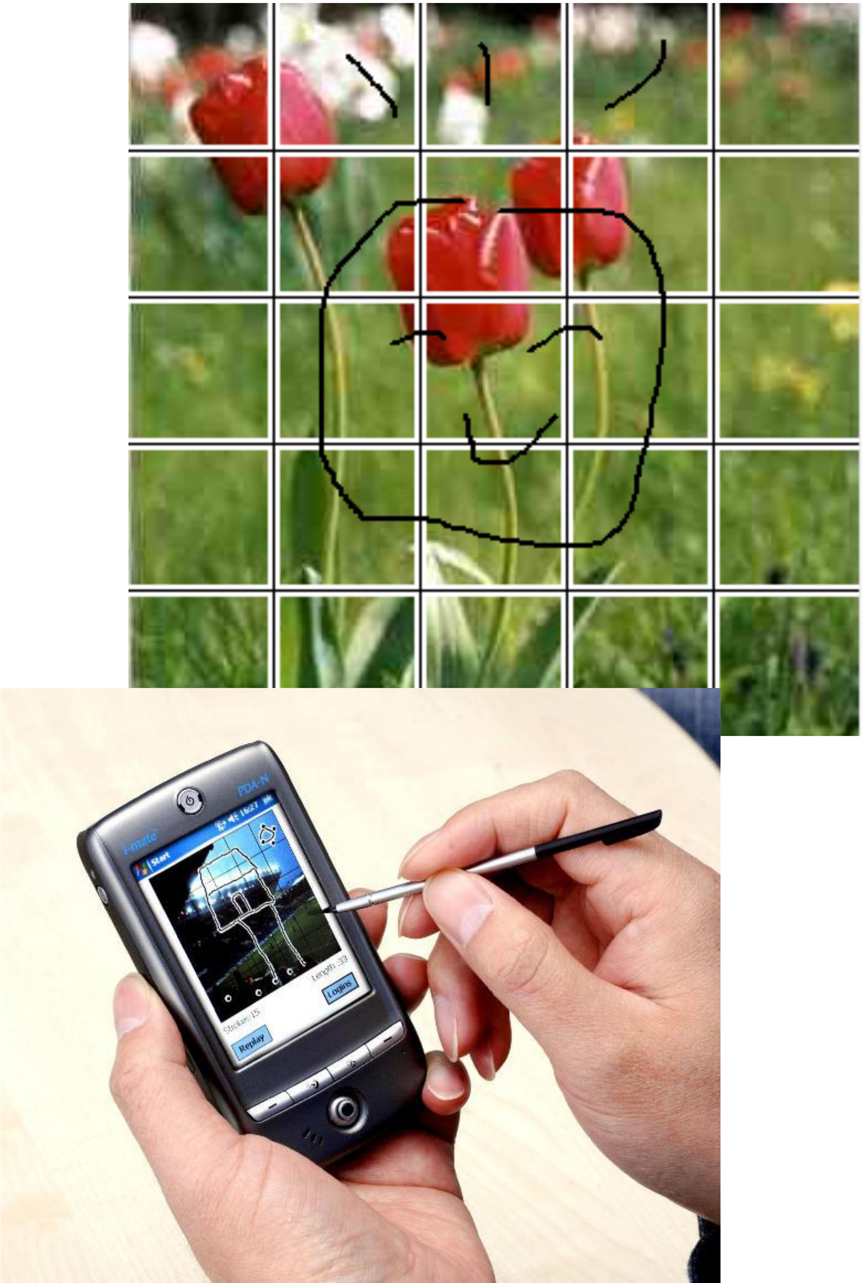
Alternative authentication mechanisms

- Example: Passfaces
- Very memorable
- … until you have more than one Passfaces password *(Everitt et al., CHI 2009)*
- *Too slow for brief tasks (Brostoff & Sasse, HCI 2000)*
- Selection biases result in low guessing difficulty (Montrose & Reiter, USENIX 1999)

Draw-a-Secret & BDAS



Yan et. al



More ‘usable’ authentication ...

- Authentication via Rorschach inkblot tests
- Singing your password *(Reynaud et al., NSPW 2007)*
- Thinking your password (free EEG thrown in - *Thorpe et al., NSPW 2005)*
- Schneier: fMRI would be cool
- Ringing up your friends in the middle of the night, asking them to find their credential for logging into a system which will reset your account *(Schechter et al. CHI 2009)*

It’s usability, Jim, but not as we know it

- Treating humans as components that can be controlled by policy. *(“If only they would make the effort to understand how to use security controls properly!”)*
- Sticking ‘better user interfaces’ on the same security controls, instead of re-examining the mechanism
- Standard mechanisms instead of ‘fitting’ security controls with user goals and values, tasks and workflows, physical and social context

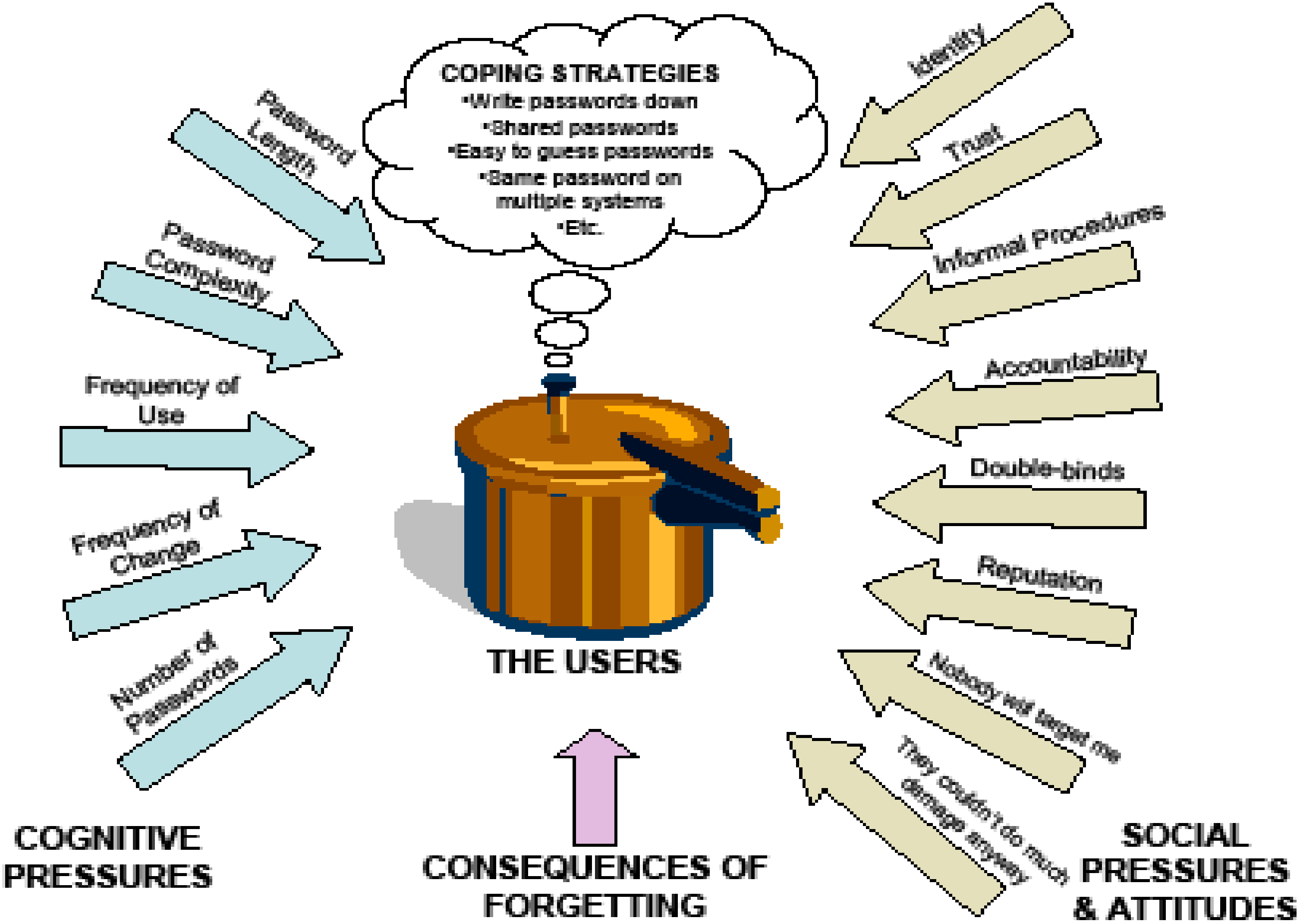
Finally, people are waking up to the cost …

- *“Security people value users’ time at zero.”* (Herley NSPW 2009)
- “*If only security managers understood the true costs for users and the organisation, they would set policies differently”* (Inglesant & Sasse, CHI 2010)
- *“CAPTCHAs waste 17 years of human effort every day” (*David Pogue, Scientific American, March 2012)

The burden of security tasks on users …

PAS

- ‘A tale of two laptops’
- Spending 30 mins/day logging in
- Spending 2 hours/month updating passwords
- Having to create 4 passwords p.a. for systems accessed 1-2 p.a.



COPING STRATEGIES

- Write passwords down
- Shared passwords
- Easy to guess passwords
- Same password on multiple systems
- Etc.

Password Length

Password Complexity

Frequency of Use

Frequency of Change

Number of Passwords

COGNITIVE PRESSURES

THE USERS

CONSEQUENCES OF FORGETTING

Identity

Trust

Informal Procedures

Accountability

Double-binds

Reputation

Nobody will target me

They couldn't do much damage anyway

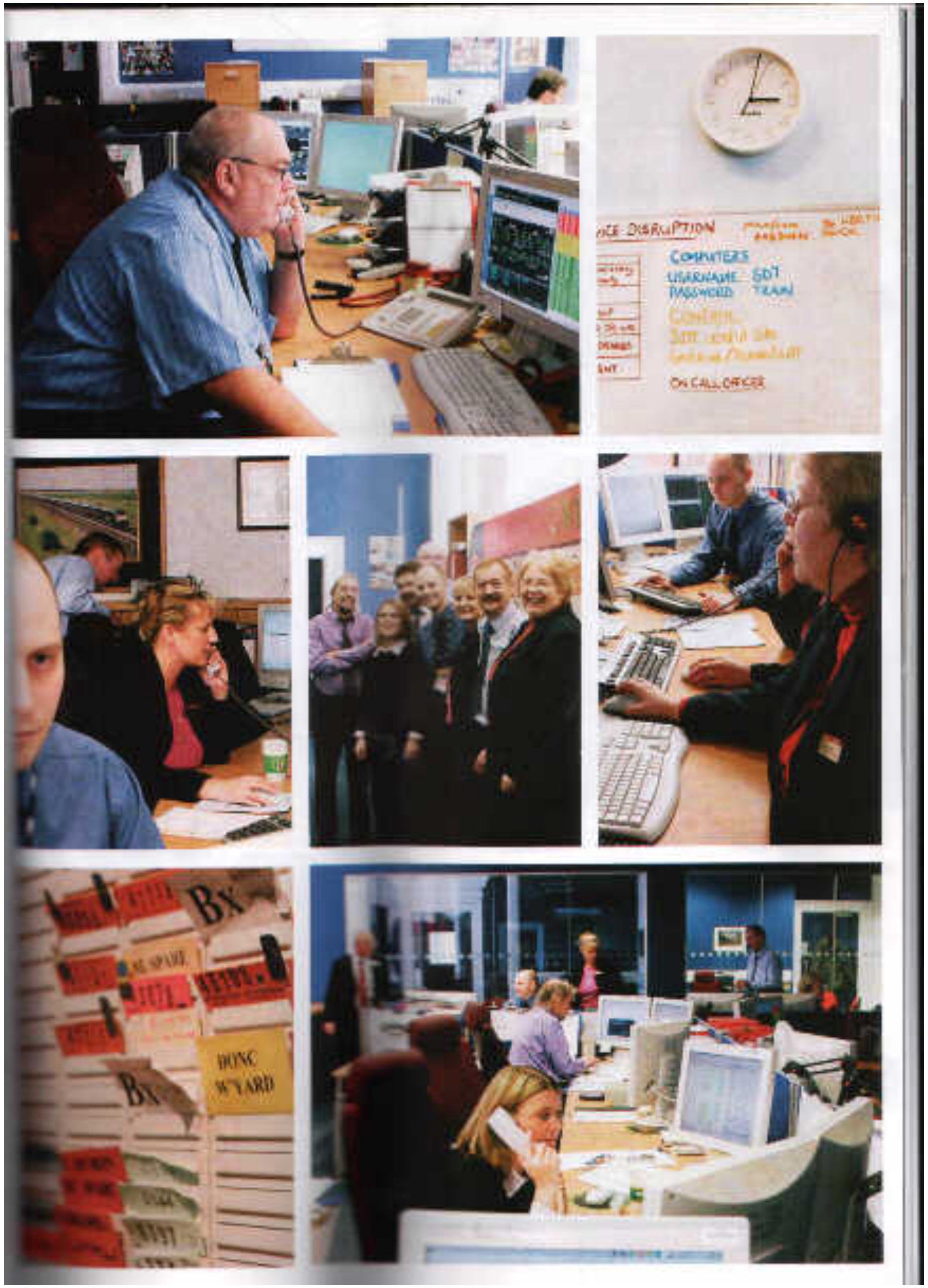
SOCIAL PRESSURES & ATTITUDES

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

… workarounds and coping strategies

- Password re-use
- Passwords stored in browsers, email folders, password managers
- Mouse-jigglers and dipping birds to disable screen locks
- Copying and emailing access-controlled documents
- ….

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



Disruptive security

- security mechanism prevent/delay completion of primary tasks
- users left to resolve conflicting primary/security task requirements
- result: friction
- … and the tolerance for that is limited

The Compliance Budget

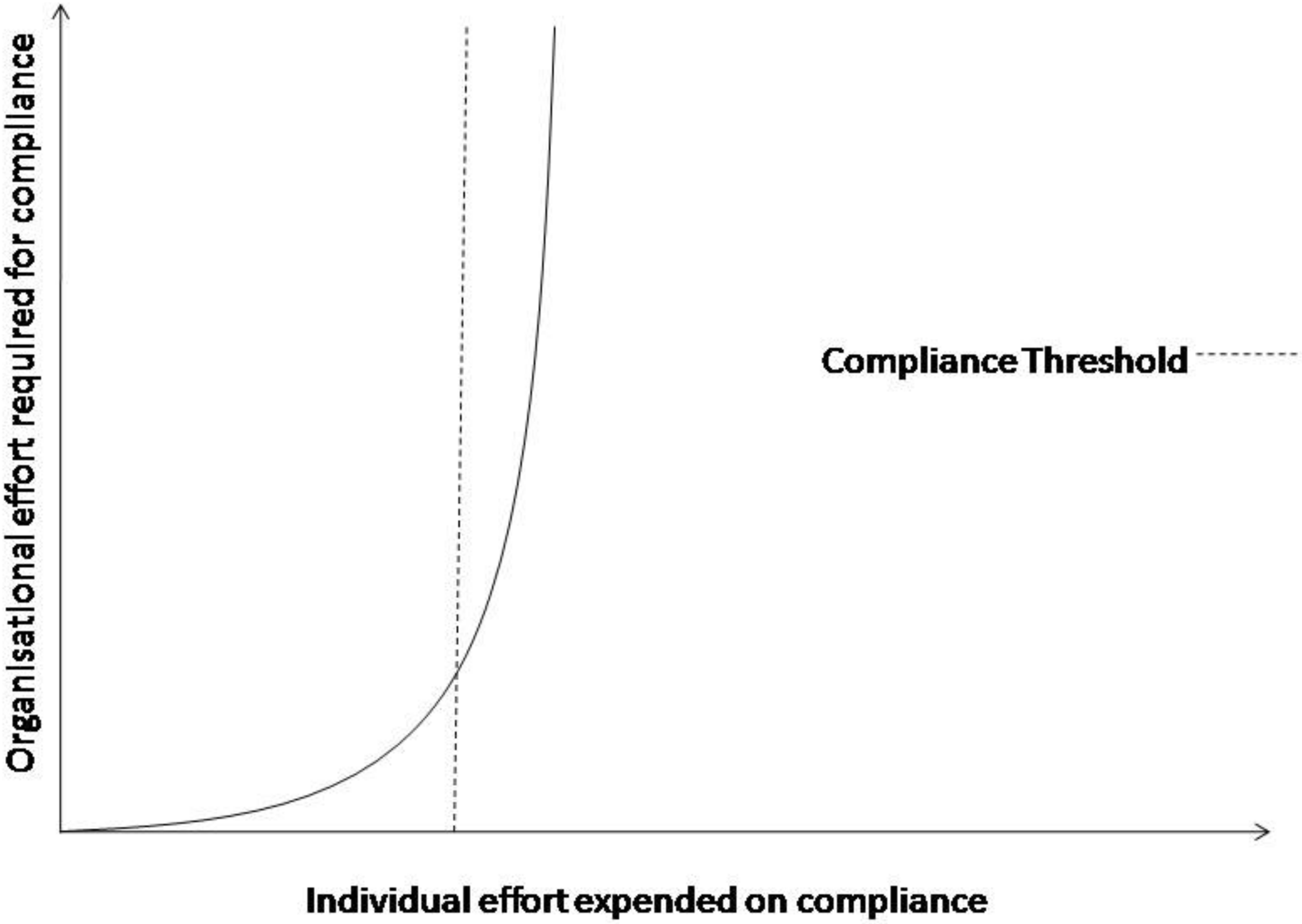
- Explains how employees make compliance decisions
- Based on interviews with employees and security managers in organisations
- Extracted cost/benefits of individual security tasks (passwords, encryption, patches)
- Perceived cost to the user more important than measurable cost
- Perceived load accumulates over tasks ...

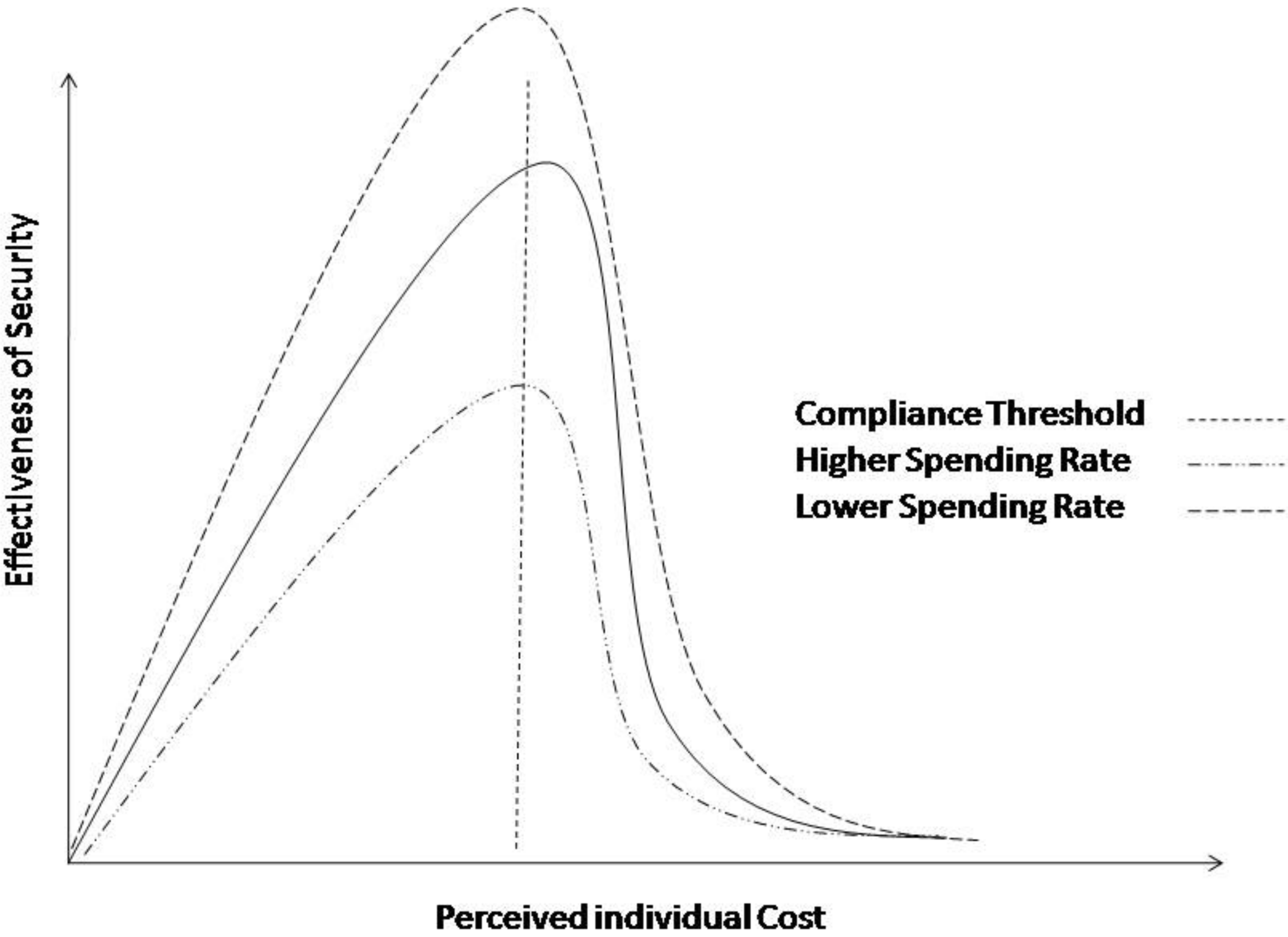
A. Beautement , M. A. Sasse & M. Wonham, The Compliance Budget Procs. NSPW 2008

Trade-off: Perceived costs/likelihoods

- Effort
  - Physical workload
  - Mental workload
- Interference with primary task
  - Failure costs
  - Delay costs
  - Restart costs

- Risk to themselves
  - Risk to productivity
  - sanctions
- Risks to organisation
  - Financial loss
  - Reputation
- Perceived likelihood of these

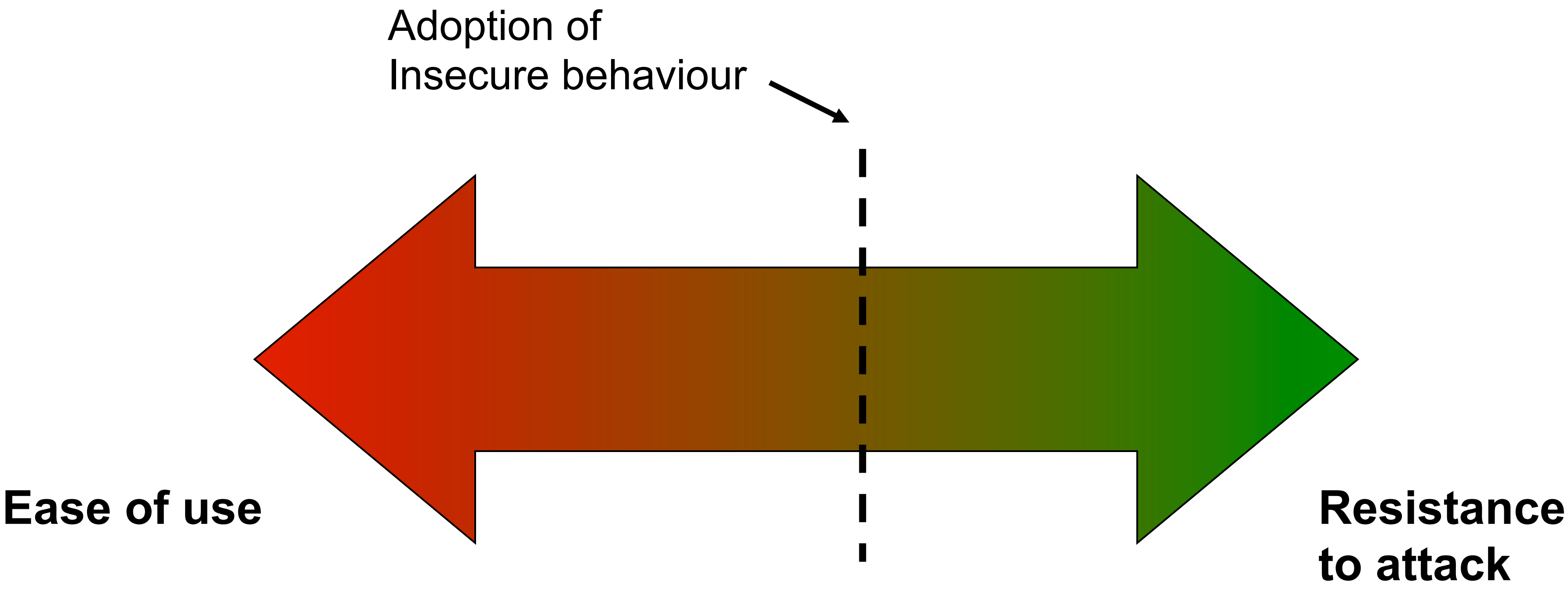

Organisational effort required for compliance
Compliance Threshold
Individual effort expended on compliance


Effectiveness of Security
Compliance Threshold
Higher Spending Rate
Lower Spending Rate
Perceived individual Cost

Longer-term impact on business

- Not answering email from home
- Not having/taking a company laptop
- Not collaborating with externals/other organisations
- Leaving the organisation

The Operating Point



Adoption of
Insecure behaviour

Ease of use

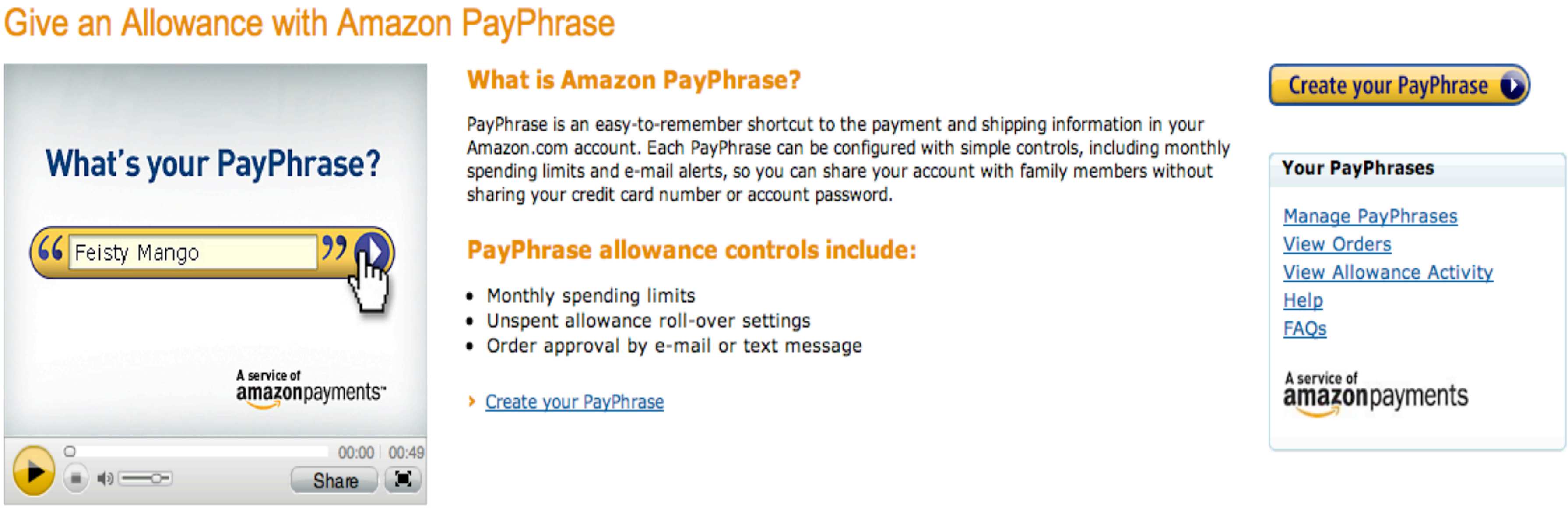
Resistance to attack

Ongoing work: lab-based studies with modified NASA TLX to measure perceived effort and disruptiveness, id operating point

Conclusions

- User compliance underpins virtually all security systems
- Increasing workload and leaving users to resolve conflicts lowers both productivity and security
- The way forward
  - Security decision-making informed by economic thinking and empirical evidence
  - Usable security by design: integrate security at the design stage, using personas and use cases

Usability by Design – Amazon payphrase



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

Your PayPhrases

Manage PayPhrases
View Orders
View Allowance Activity
Help
FAQs

Example: authentication

- Less authentication
- Different mechanisms for different user capabilities and preferences, task (frequent and infrequent usage!), and contexts
- Move towards implicit authentication
  - Learning from e-commerce: recognise users through cookies, history/patterns, etc.
  - using tokens or biometrics (“0-Effort, 1-step, 2-Factor authentication”) – e.g. Touché system
  - exploit modality of interaction – touch on touchscreens, video, audio

Good security designers used to know this …

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.