What would user-centred security look like?

M. Angela Sasse

Professor of Human-Centred Technology &

Head of Information Security Research

Department of Computer Science

University College London, UK

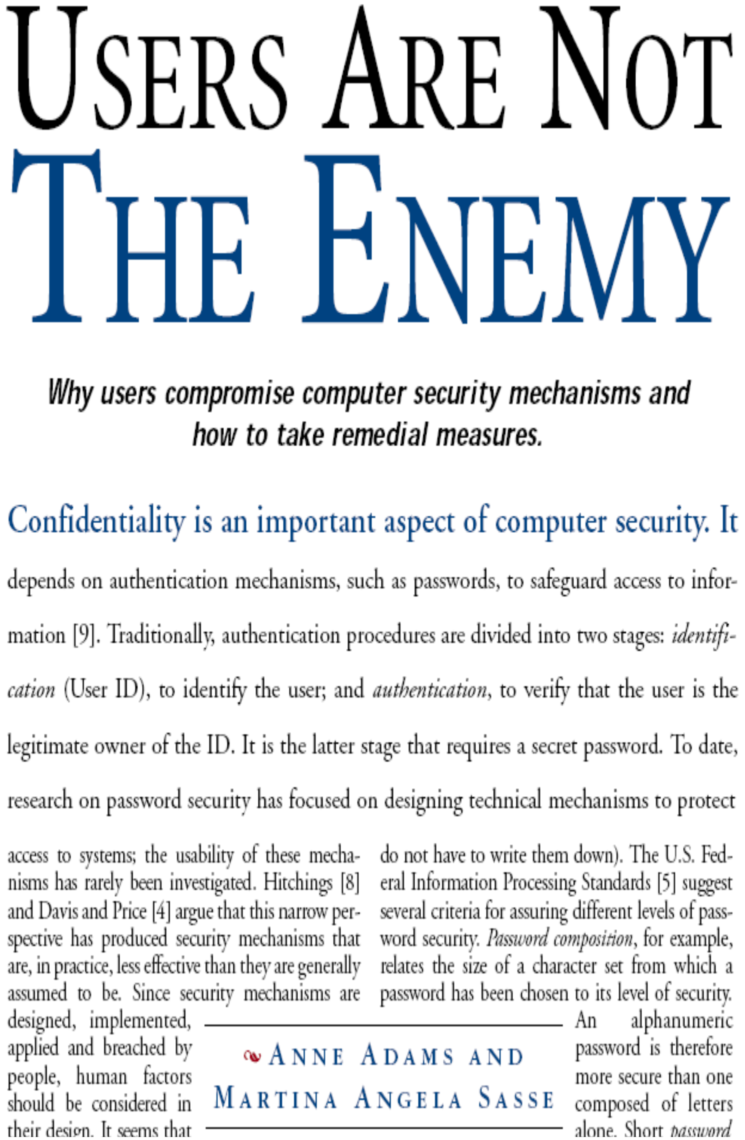
www.cs.ucl.ac.uk/staff/A.Sasse

Why is usability important for security?

- Results of failure to make security usable are much more widespread than generally realised
- Users: errors, frustration, annoyance, individual losses
- Organisations:
  - losses from risks: systems, cash, customers, reputation
  - impact on business processes and performance
- Society:
  - security seen as an obstacle/annoyance, not something to be valued
  - successful attacks undermine trust and confidence

How did I get into this?

- Study on password problems at BT Labs
- User workload too high
- Short-cutting security mechanisms
- Don’t understand risks
- War between users and security department



Users Are Not The Enemy

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

Anne Adams and Martina Angela Sasse

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*

Framework for usability

- Users/actors
  - Individual: employee, customer, citizen, parent, …
  - Collective: companies, government
- Activity
  - Goals of interaction: WHAT
  - Tasks/processes carried out to achieve goals: HOW
- Context of interaction
  - Physical
  - Situational
  - Cultural
- Plus: capability system/technology platform

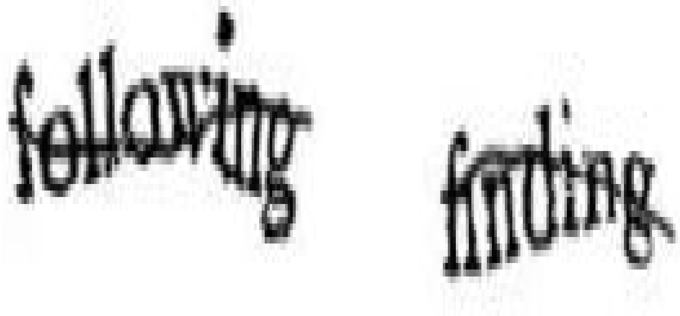
Users

- Understand requirements and capabilities of users
- General capabilities and requirements
  - Human memory, error, fatigue, biases …
  - But also: what are they trying to achieve (→ goal)
- Specific capabilities and requirements
  - Security provides access to services: must not exclude user groups with specific requirements

Activity

- Security is a *secondary* or *enabling* activity
- User's perspective:
  - at best: slows down security completion of task
  - at worst: prevents them from achieving their goal
- Organisational perspective
  - at best: security consumes resources, slows down business process
  - at worst: stops business processes
- Business processes and user tasks impose performance requirements on security tasks

Examples

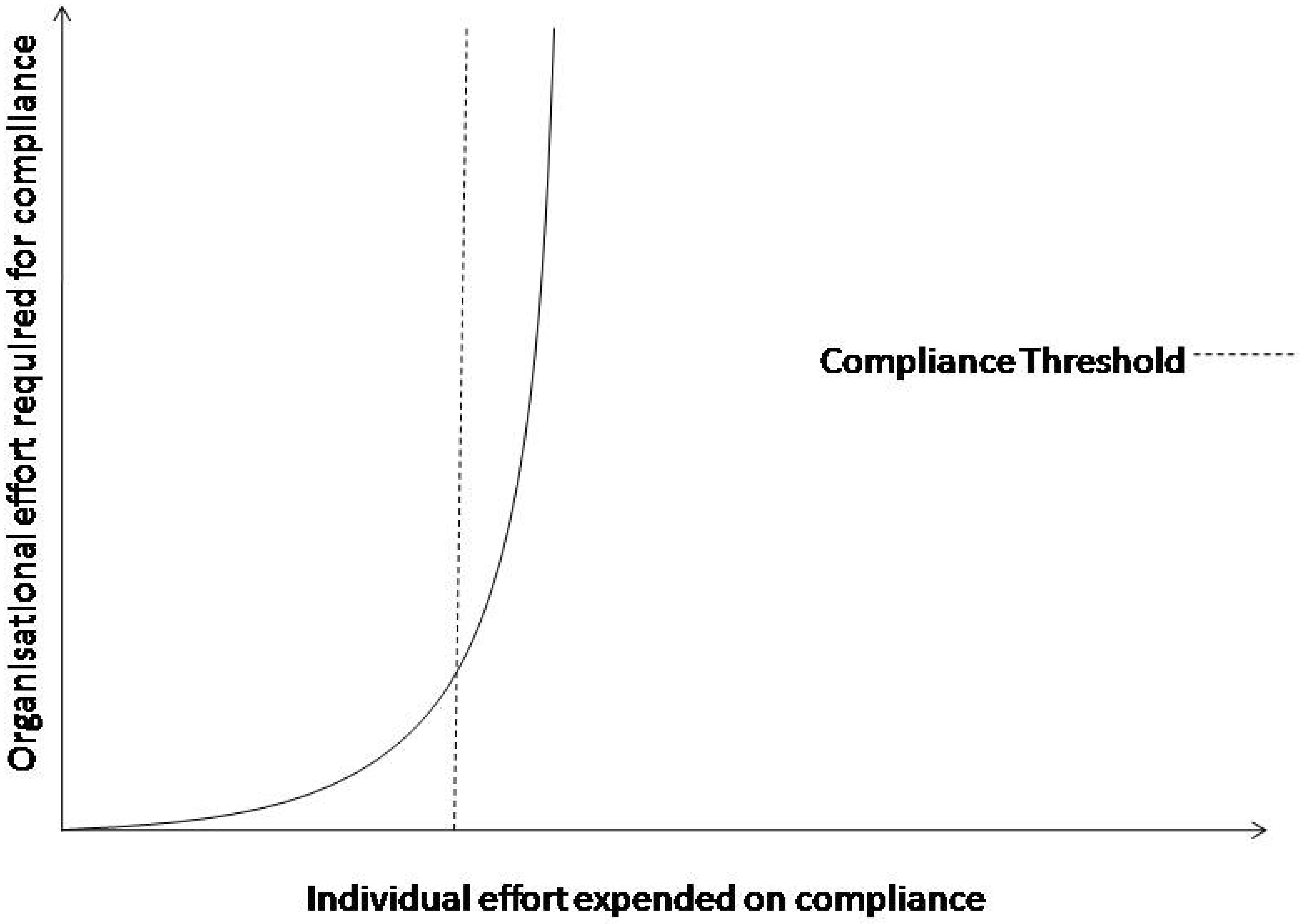


Context

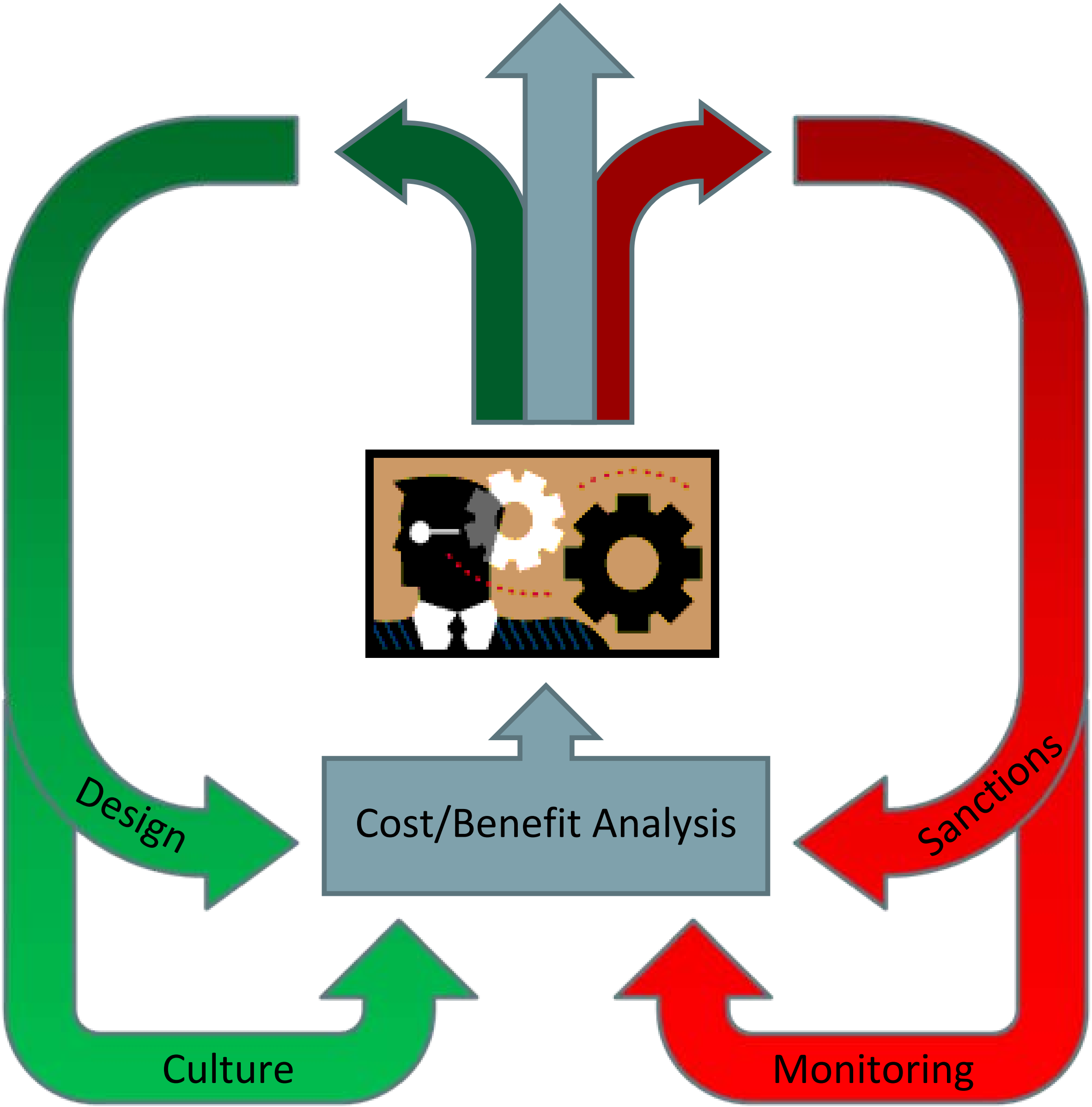
- Physical
  - indoor/outdoor: temperature, lighting, pollution, …
  - public/private:
- Situational
  - Impact of interaction or failure on individual and others
- Cultural
  - Behavioural norms: e.g. acceptability of touching equipment, “not allowed to smile”

Cost vs. Benefits of Security

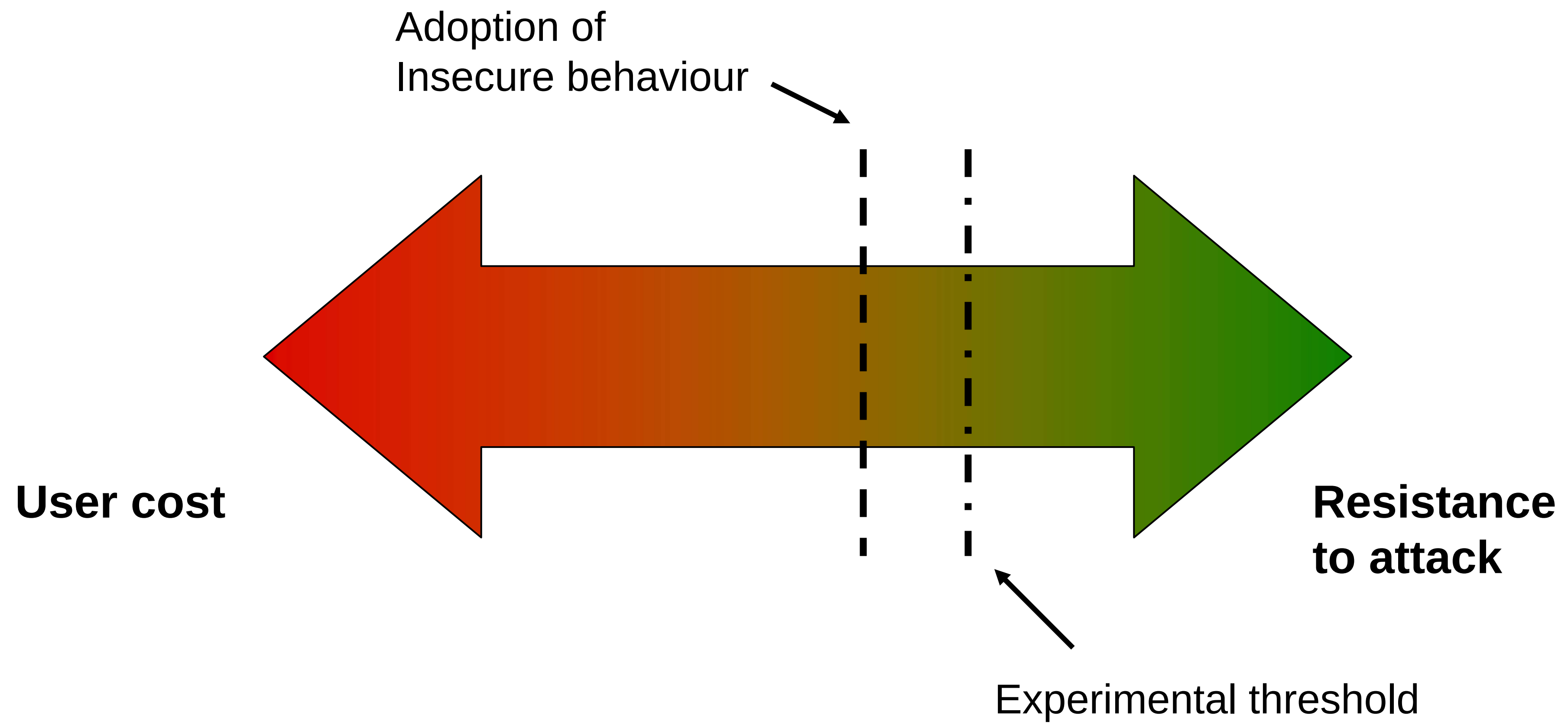
- Individual costs
  - Physical workload and mental workload
  - Actual and perceived costs
- Organisational costs
  - Cost of operation (including training and repair)
  - Failure cost
  - Impact on business process
  - Impact on employee behaviour, trust, goodwill, …


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

Compliance Decision



Trade- offs



Adoption of
Insecure behaviour

User cost

Resistance
to attack

Experimental threshold

Key research challenges

- Identifying and understanding trade-offs
- Need to be able to quantify and compare costs for different usability and security criteria, and stakeholders
- Identifying and reconciling individual and collective goals
- Understanding short and long-term impact on individuals, businesses and society