IBM BusinessConnect
Realise the art of the possible.

Security Track hosts

Peter Jopling, Business Unit Executive IBM Security Systems

Roger Gate, Business Unit Leader, Security and Privacy Services

IBM BusinessConnect
Realise the art of the possible.

Making Security More Productive

M. Angela Sasse
University College London, UK

Professor of Human-Centred Technology
Head of Information Security Research
Department of Computer Science, UCL
Director, Research Institute for Science of Cyber Security
www.ucl.ac.uk/cybersecurity/

Overview

Case History: the Great Authentication Fatigue and its consequences

Why most usable security research is misguided

Can alternatives work – e.g. FedID?

Outline of a new design approach

- Divide and conquer: different solutions for different contexts
- Smarter technology, thought-through implementation

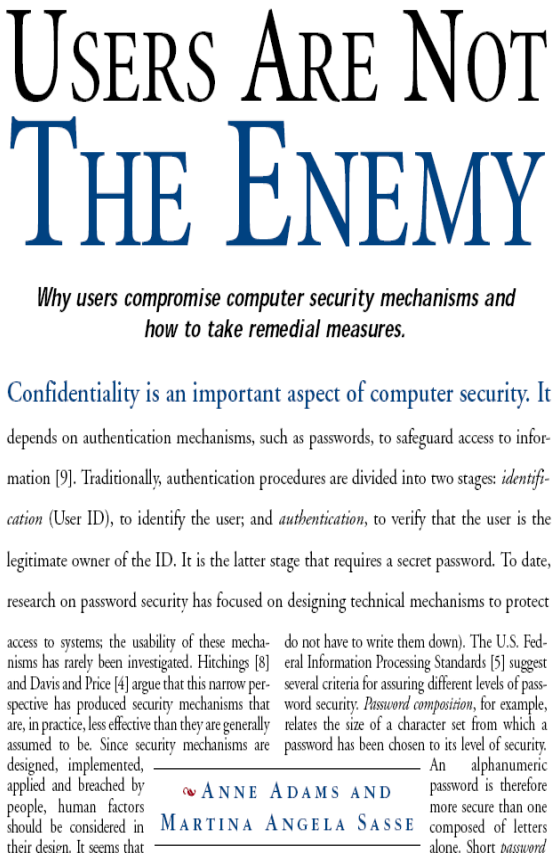
How it all began …

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

The experts didn’t see the problem

Nielsen (2000) said that biometrics are highly usable and would replace passwords.
Schneier (2000) and Gates (2004) predicted that passwords would become obsolete.

Instead, today ….

People have more passwords.

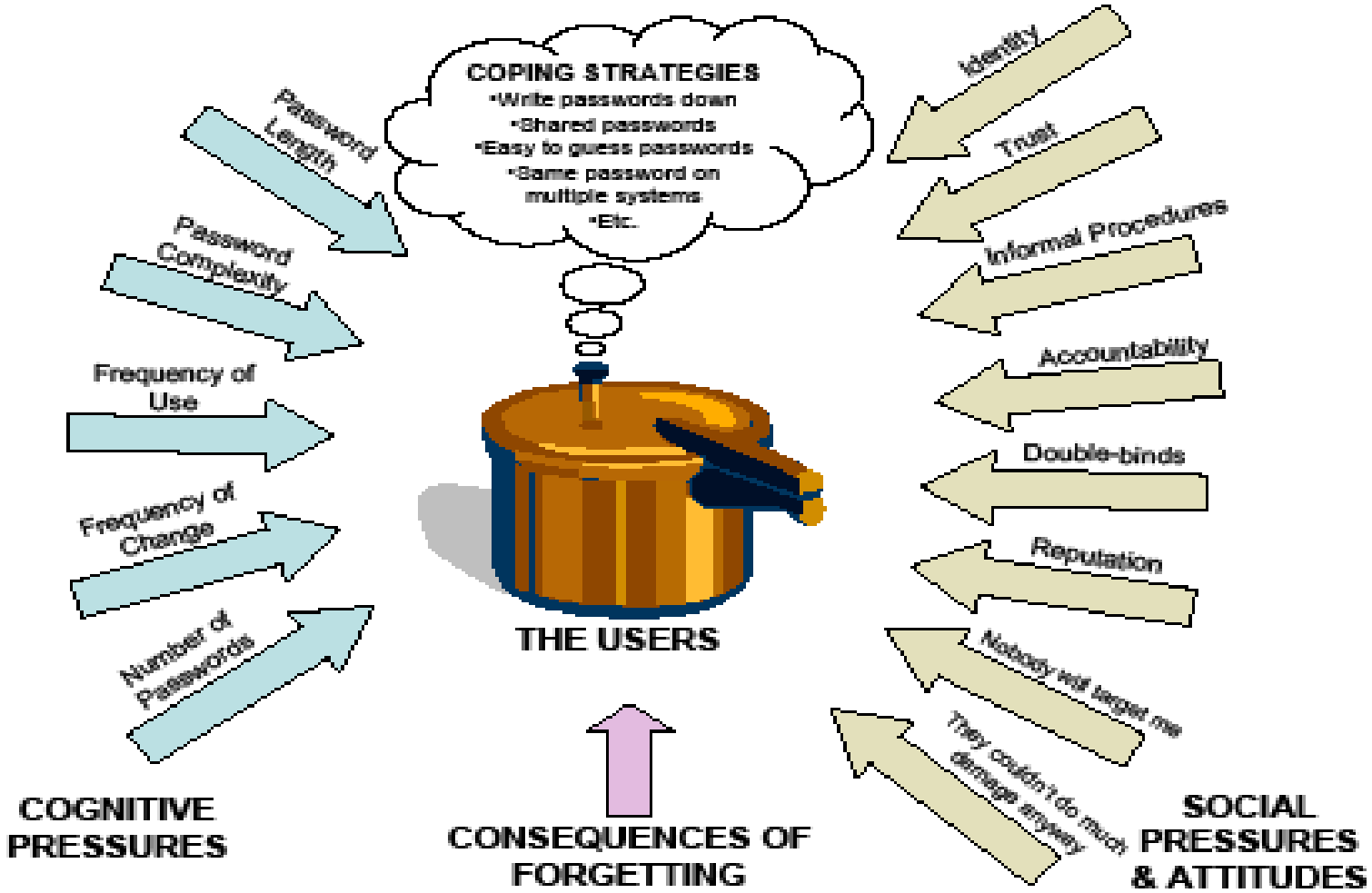
Longer ones.

With more restrictions.

They write down, store, re-use and re-cycle passwords across accounts and devices, and share them with others.

They have to create and recall back-up credentials to re-set passwords.

And solve a CAPTCHA (the anti-usability devil incarnate) before they even get to the re-set ...



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

The burden of authentication – consequences

Immediate impact: productivity loss

Support costs

Security vulnerabilities

Creating/reinforcing negative attitude to security

What are the longer-term implications?

Insights from study for NIST, and studies in corporate environments

Results

Frequency: On average, employees authenticated 23 times/day (ranging from 4 to 40)

Failure rate: 529 authentication events, there were 49 problems (9.3%)

Most common causes of these problems were:

- Mistyped passwords (49%)
- Wrong passwords used (14%)
- Unknown cause (14%)
- Forgotten usernames (4%)

Most authentication events caused mild-moderate frustration

Key insights

Authentication is a significant drain on productivity

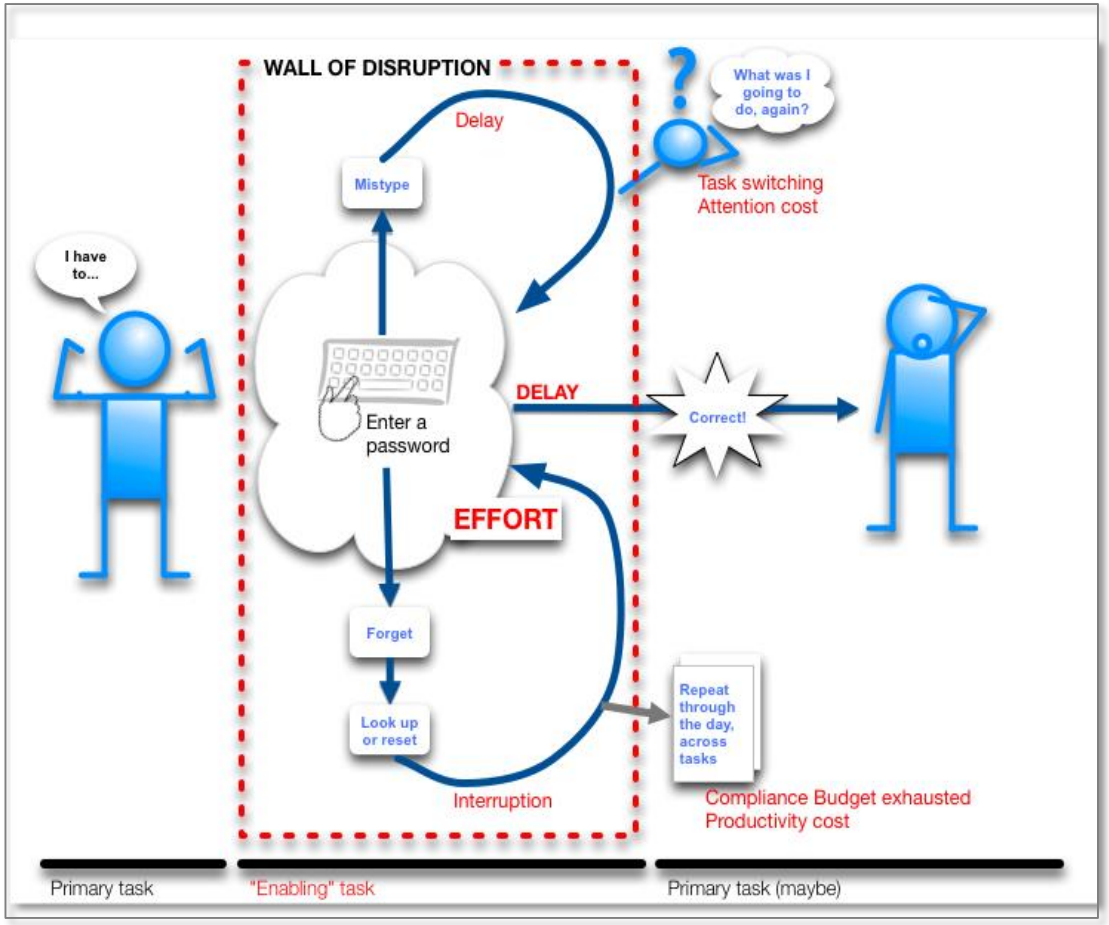
- not just the time spent, but *disruptiveness* on primary task
- the more complex the authentication task, the higher the cost of task-switching

Examples of productivity effects

“For the email, when I was at home, if I don't do anything on the Web page for five minutes or 10 minutes, it will log me out automatically. Which that can get frustrating because then I have to close the browser, open it up again, use the RSA key, hope I get it right the first time. And I can do that 15 or 20 times throughout the day. And a lot of times I'm just so tired of re-logging in, I'll just stop checking my email. I might do it once every three or four hours instead of every 20 minutes.”

“… there are lots of things that harm productivity, such as the inconvenience associated with working from home. I would probably do more work from home if there weren't so many security issues associated with that.”

Authentication as a ‘wall of disruption’



The Authentication Hate List

Repeated authentication to the same system (e.g. because of 15 min time-outs)

“Well, I think that if I just logged in, then it should be able to understand that I just logged in and not ask me for the password again. […] That's too much, because you shouldn't have to do extra work to authenticate. Because yeah, it can just pick up what you do.”

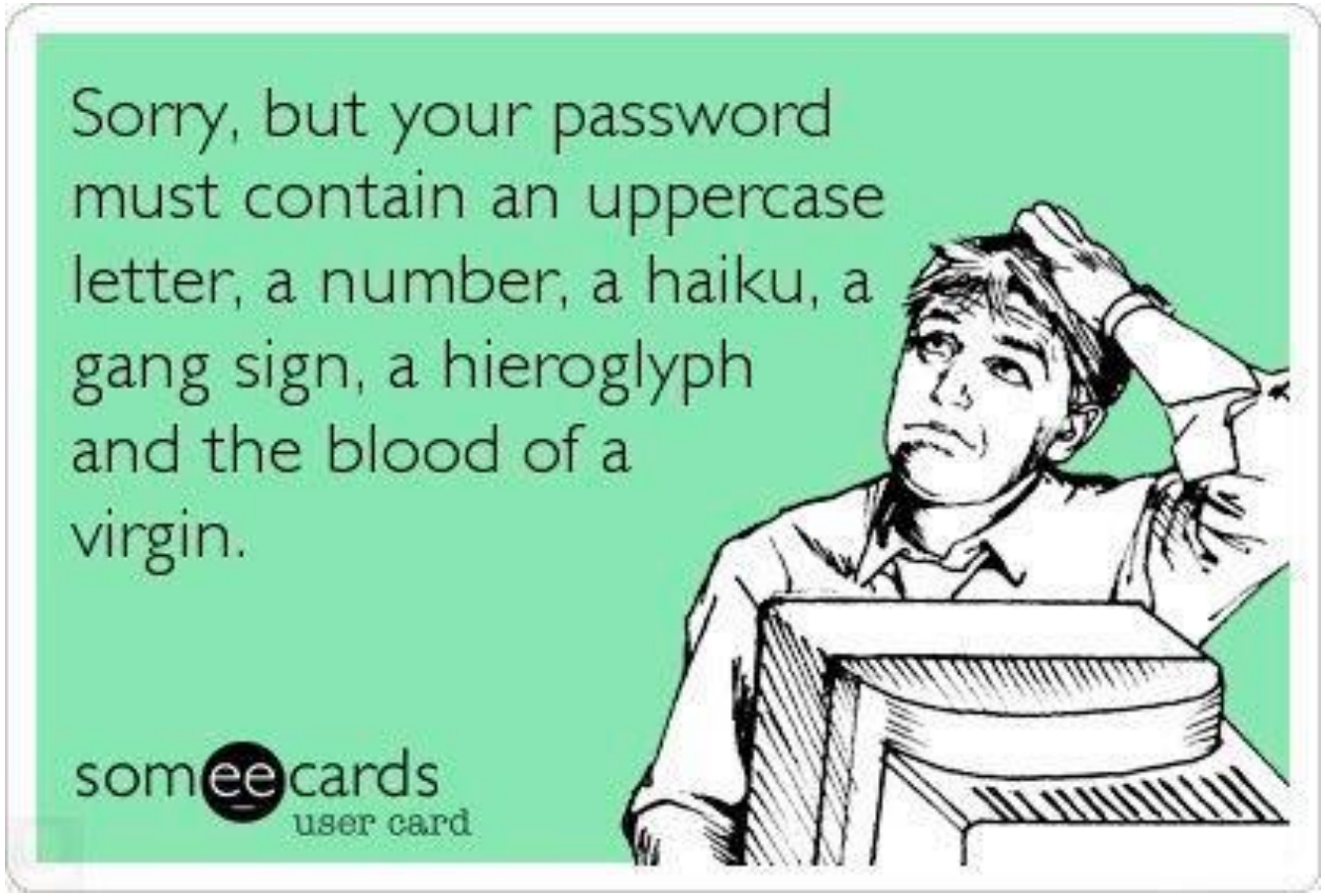
Authentication Hate List

Repeated authentication to the same system (e.g. because of 15 min time-outs)

Authenticating to infrequently used systems

- Difficulty to recall previous password
- Password could have expired in the meantime
- Resetting a password is not easy

Creating a valid password (different rules for each system)



http://humourspot.com/wp-content/uploads/2013/04/Sorry-but-your-password-must-contain....jpgcontent/uploads

Authentication Hate List

Managing a large number of different credentials

Different policies means user strategies for creating & recalling pws don’t work

Which credentials to use for which system

Use of RSA tokens

“It's this extra, again, effortful stuff. I have to dig around in my bag and get the RSA ID token out and then set it on my laptop and then type out the number, make sure that you're not typing it right before changes or as it's changing or whatever.”

Employees’ coping strategies

Batching and planning of activities to limit the number of logins

Storing passwords or writing them down

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

Employees’ coping strategies

Batching and planning of activities to limit the number of logins

Storing passwords or writing them down

Resetting passwords to the same one

Creating passwords to be memorable

Creating passwords that are easy to type on mobile devices

Maladaptive coping strategies

Giving up devices:

> *“If I had a company laptop I would have to log in twice, once when you turn it on because the hard drive's encrypted, and then again to actually get into Windows or the operating system. […] So I never wanted a company laptop for that reason. I don't want to have to log in more times than I need to.”*

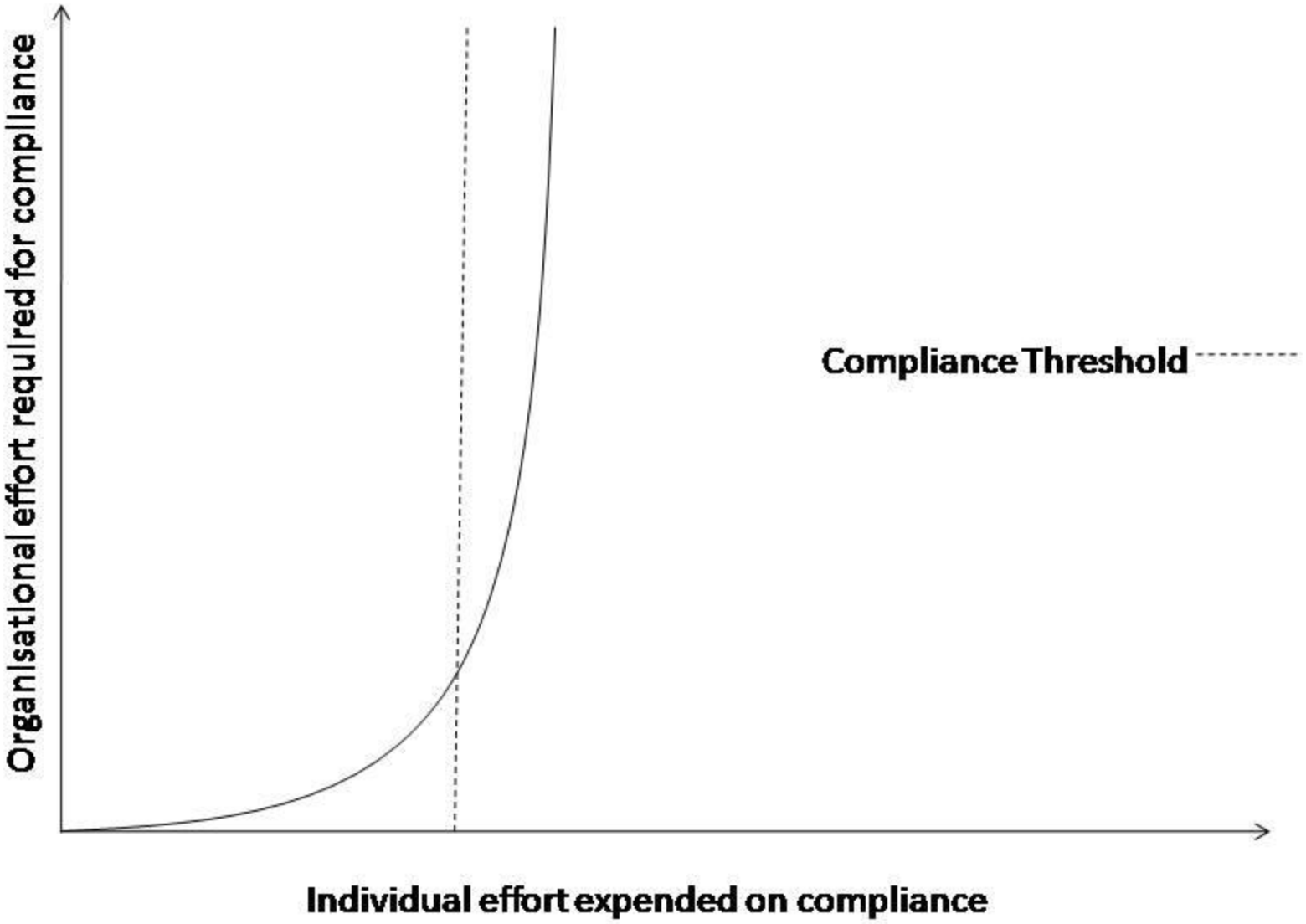
So many employees stop taking laptop when travelling – or give it back altogether

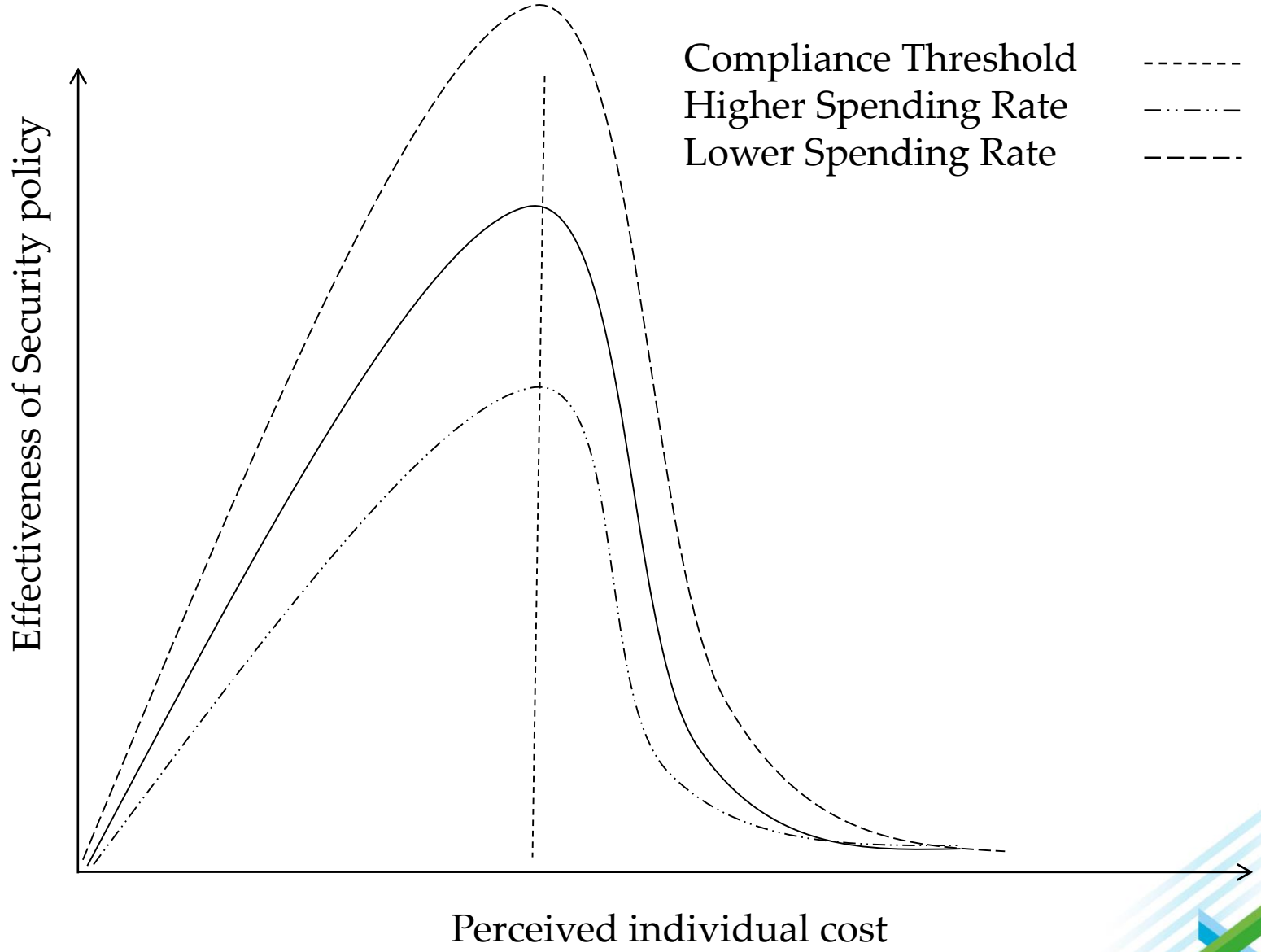
Maladaptive coping strategies

“I have research collaborations with people in other institutions, but it is just extremely difficult to share files with them, to transfer software you're writing, and that sort of thing. To me, the way that security impacts work is not that I waste a few seconds typing in a password, but it is these things that you just can't do because of the limitations of security policy. […] I can think of cases when I have thought it would be really nice to include some person at another university on a software development project, but then I realize it is going to be such a tremendous pain to organize that.”

The ‘Compliance Budget’

Beautement, Sasse, Wonham
NSPW 2008




Compliance Threshold
Higher Spending Rate
Lower Spending Rate
Effectiveness of Security policy
Perceived individual cost

Conclusions

Users try hard to cope with authentication, but it just compromises their productivity too much.

Users are not comfortable with breaking rules, but feel they have no choice. (Companies collude, but leave users with guilt.)

There is an increasing sense of exasperation:

“Technology should be smarter than this!”

Obstacle security = unproductive security

Making Security More Productive

Fit into individual goals and business processes, rather than creating obstacles.

Example: 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

Making Security More Productive

Fit into individual goals and business processes, rather than creating obstacles.

Fit to the device (keyboard vs. touch) and exploit modality and data already used (voice/video, cookies, etc.)

Before chosing a security measure, consider other business needs – what else can security do for the process?

Questions?

Acknowledgements: Password Burden Study

Dana Chisnell (UsabilityWorks)

Kat Krol (UCL)

Michelle Stephens and Mary Theofanos (NIST)

Acknowledgements: FedID 4 gov Study

Sacha Brostoff, Charlene Jennett and Miguel Malheiros (UCL)

Thank You!