# *Busting The Myth Of Dancing Pigs: Angela's Top 10 Reasons Why Users Bypass Security Measures*

*M. Angela  Sasse*

**Professor of Human-Centred Technology,**

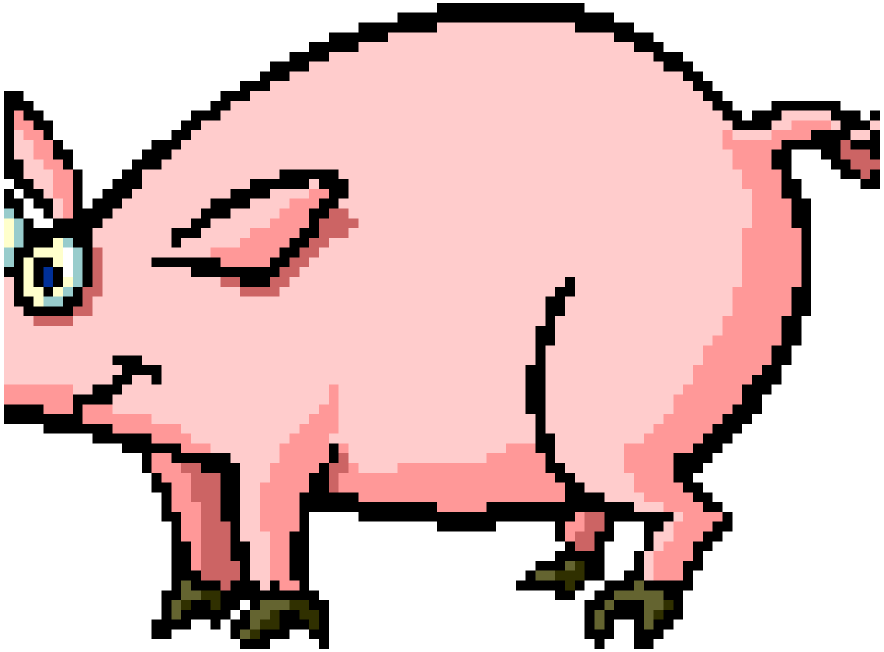
**Head of Information Security Research**

**Director, Research Institute for Science of Cyber Security**

**University College London, UK**

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

# Dancing Pigs



*“ Given a choice between dancing pigs and security, users will pick dancing pigs every time. ”*

Gary McGraw and Edward Felten: *Securing Java* (John Wiley & Sons, 1999, Chapter 1)

# A more differentiated view …

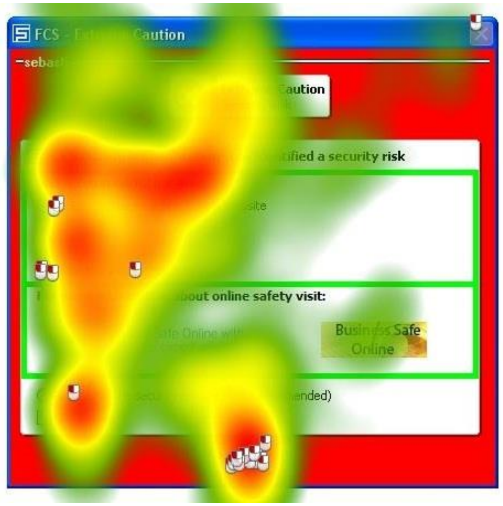
*If J. Random Websurfer clicks on a button that promises dancing pigs on his computer monitor, and instead gets a hortatory message describing the potential dangers of the applet — he's going to choose dancing pigs over computer security any day. If the computer prompts him with a warning screen like:* "The applet DANCING PIGS could contain malicious code that might do permanent damage to your computer, steal your life's savings, and impair your ability to have children," *he'll click OK without even reading it. Thirty seconds later he won't even remember that the warning screen even existed*.

Schneier: Secrets and Lies. 2000

# Do you agree?

- *He'll click OK without even reading it.*

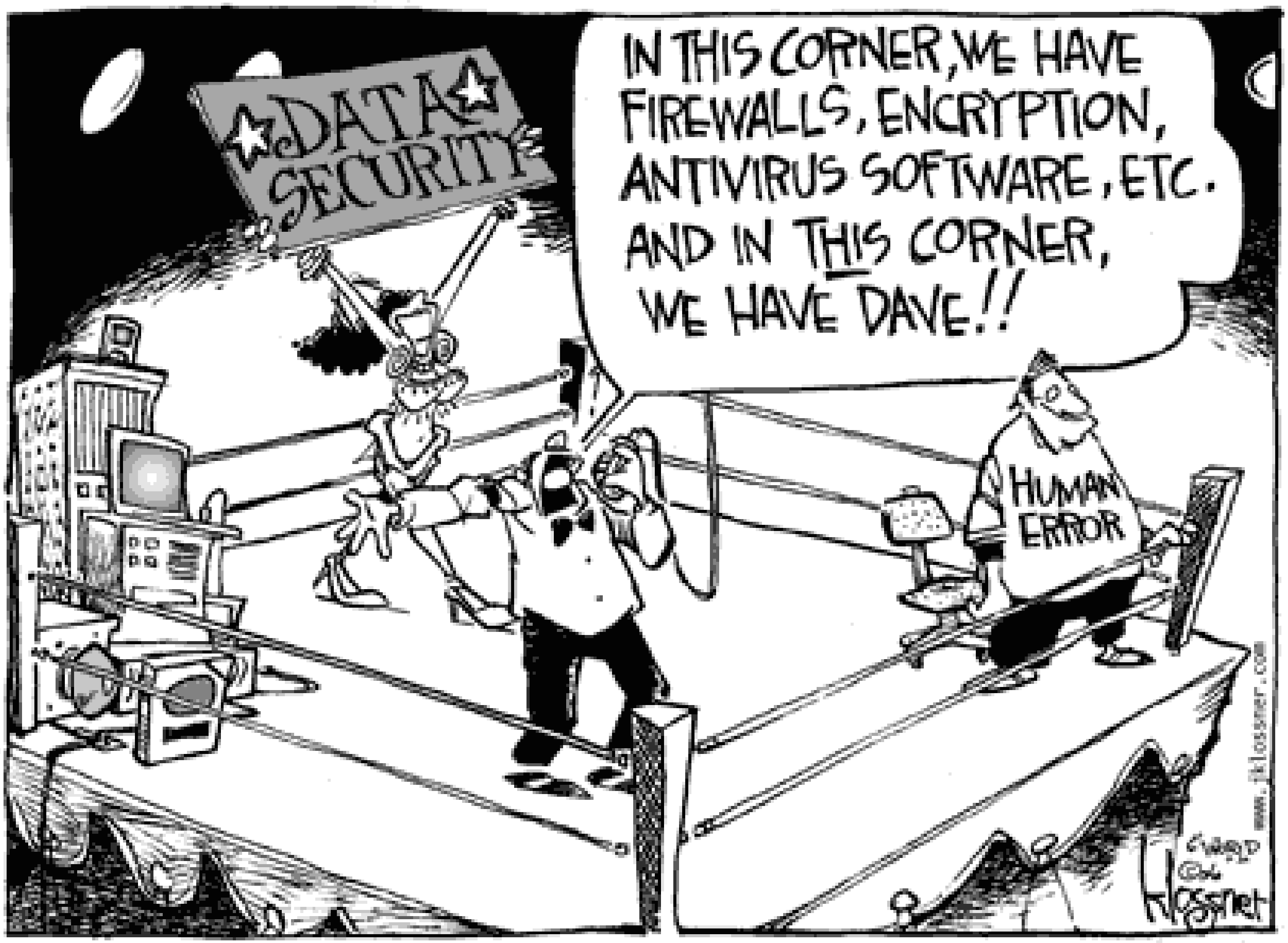
- False.



- *Thirty seconds later he won't even remember that the warning screen even existed*.

- True – but why?

# Stupid user



DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WORLD ©06 Klossner

Angela’s Top Ten:

Users don’t follow security advice because …

# 1. They don’t believe the threat is real

- Too many warnings - very few consequences.
- Language gets scarier, more clicks required to get around: and still - rarely are there consequences.
- At least not ones that are visible to the user.
- This reinforces their belief that warnings are there to be ignored.

# 2. Even if they believed you – they'd still ignore you (most of the time)

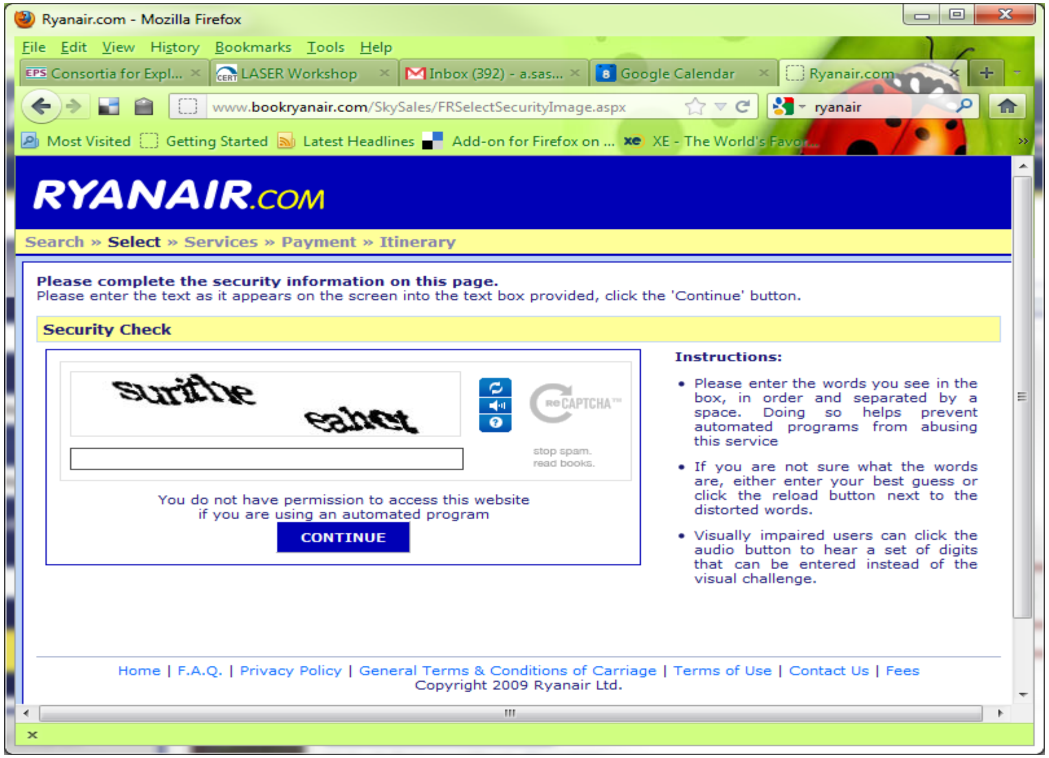
- User actions are driven by primary goals
- (Shock, horror) people do take risks – and weigh them against benefits of primary goals
- … and most users, most of the time, don't bear the cost of security problems (Cormac Herley: *So Long And Not Thanks For All The Externalities, NSPW 2013*)

# 3. You don’t give them a real choice

- Go home and pull a blanket over your head?
- Wait until a security expert comes by to help you?
- NEAT advice on warnings from Microsoft (Reeder et al.)
  - Necessary
  - Explained
  - Actionable
  - Tested
- http://www.microsoft.com/en-us/download/details.aspx?id=34958

# 4. You are asking them to do something that is humanly impossible

- for most humans, anyway
- Like: solve a CAPTCHA


Ryanair.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Consortia for Expl...
LASER Workshop
Inbox (392) - a.sas...
Google Calendar
Ryanair.com
www.bookryanair.com/SkySales/FRSelectSecurityImage.aspx
ryanair
Most Visited
Getting Started
Latest Headlines
Add-on for Firefox on ...
XE - The World's Favor...
RYANAIR.COM
Search » Select » Services » Payment » Itinerary
surithe
eahet
reCAPTCHA™
stop spam.
read books.
CONTINUE

**Please complete the security information on this page.**
Please enter the text as it appears on the screen into the text box provided, click the 'Continue' button.

**Security Check**

You do not have permission to access this website if you are using an automated program

**Instructions:**

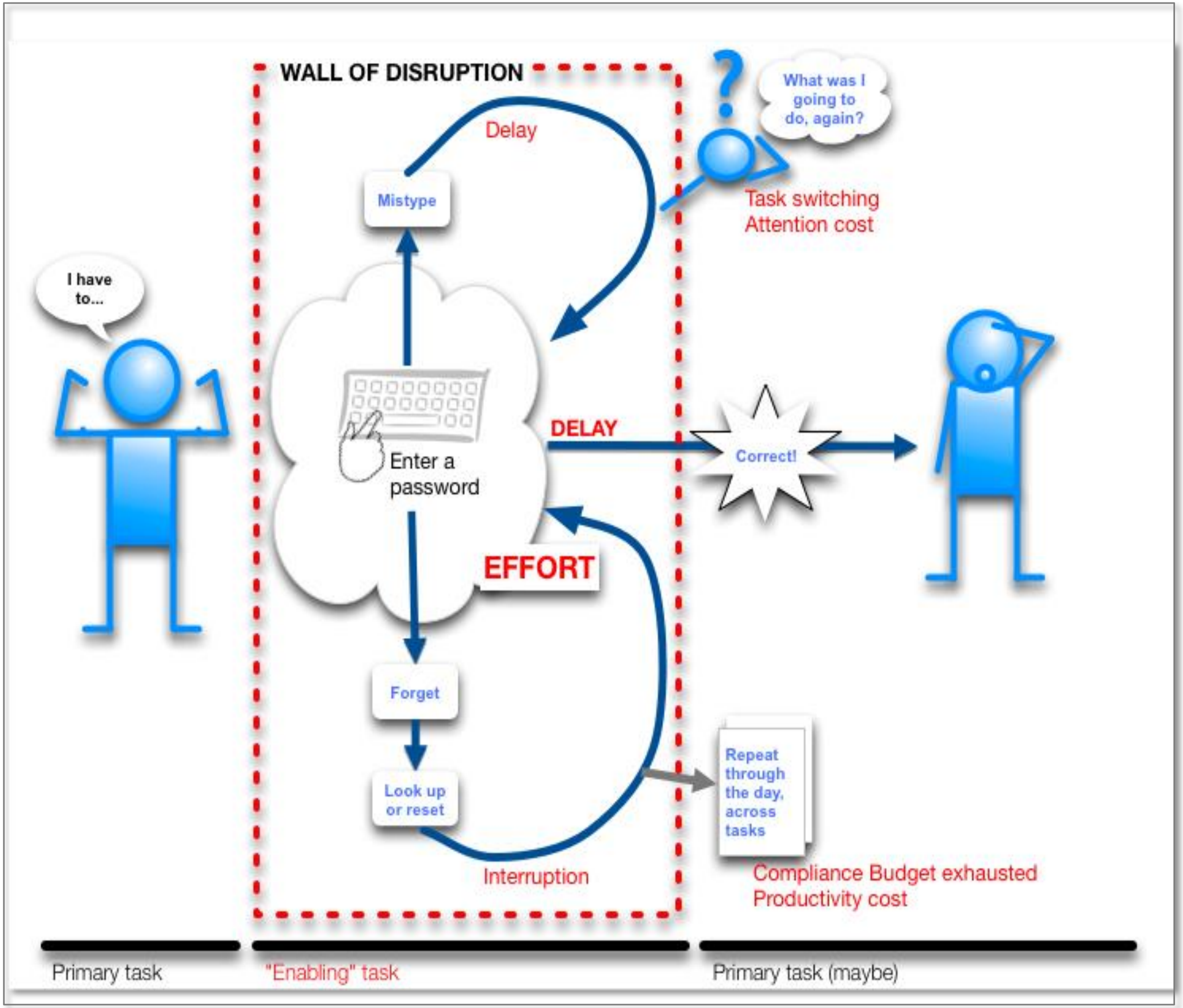
- Please enter the words you see in the box, in order and separated by a space. Doing so helps prevent automated programs from abusing this service
- If you are not sure what the words are, either enter your best guess or click the reload button next to the distorted words.
- Visually impaired users can click the audio button to hear a set of digits that can be entered instead of the visual challenge.

Home | F.A.Q. | Privacy Policy | General Terms & Conditions of Carriage | Terms of Use | Contact Us | Fees
Copyright 2009 Ryanair Ltd.

- Anti-usability: solve security problem by making every user jump a big obstacle
- Technology writer David Pogue calculated we spend 17 man-years every day on CAPTCHAs (Scientific American, March 2012)
- http://ihatewordverifications.blogspot.de/
- Accessibility issues → alternative CAPTCHA = backdoors for attackers

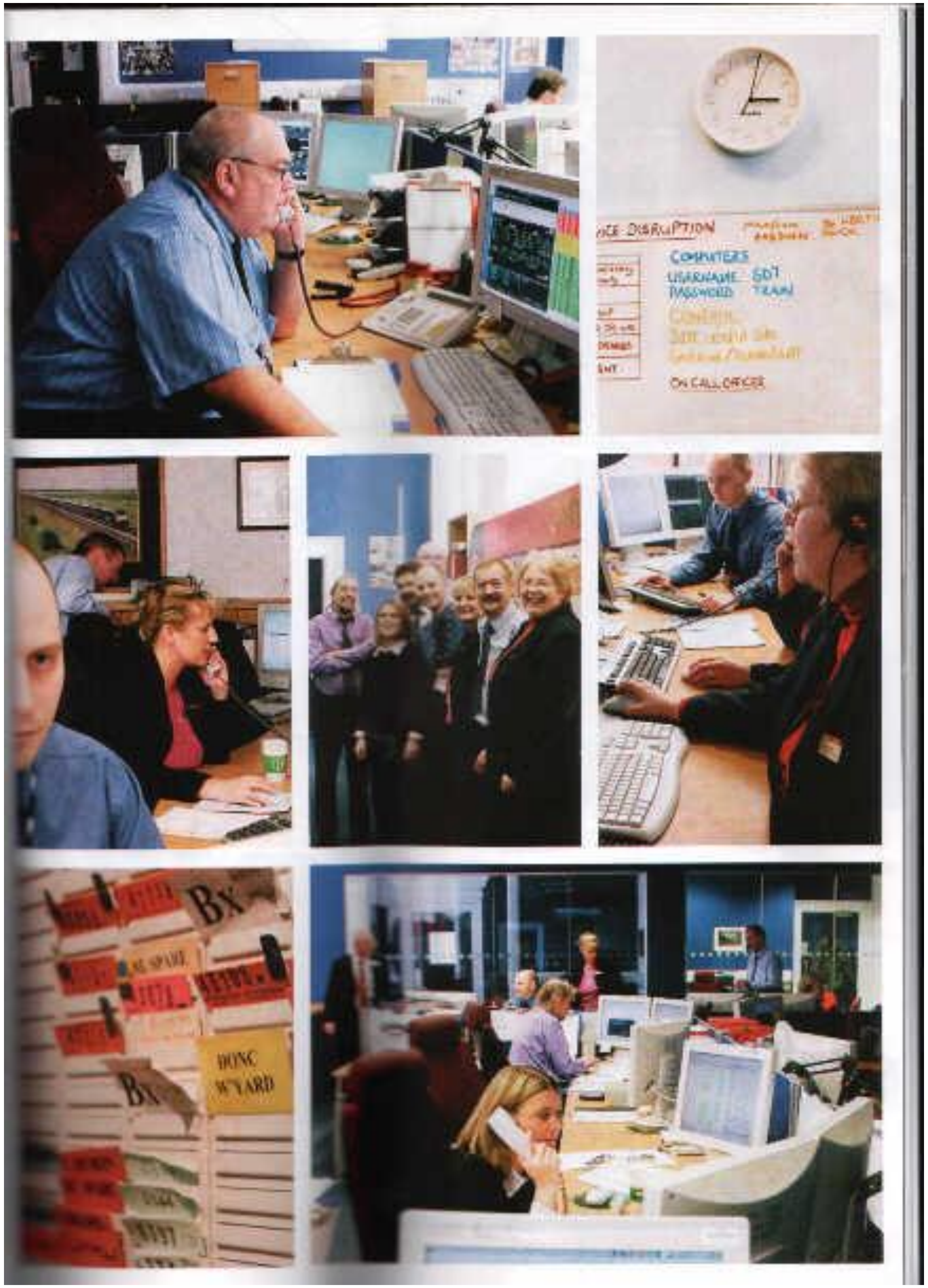
# 5. You are asking them to do something that might be possible – if they had to do it once or twice a day …

- but not 20+ times a day – welcome to *The Great Authentication Fatigue*
- users have just had it with passwords


WALL OF DISRUPTION
I have to...
Delay
Mistype
What was I going to do, again?
Task switching
Attention cost
Enter a password
DELAY
Correct!
EFFORT
Forget
Look up or reset
Repeat through the day, across tasks
Interruption
Compliance Budget exhausted
Productivity cost
Primary task
"Enabling" task
Primary task (maybe)

- Disruption for users
- Huge productivity losses for organisations
  - Re-organising work to avoid security
  - Opportunity cost
- Workarounds that undermine security
  - Widespread password re-use
  - mouse jigglers

- And externalising/sharing is so common that everyone forgets they do it …



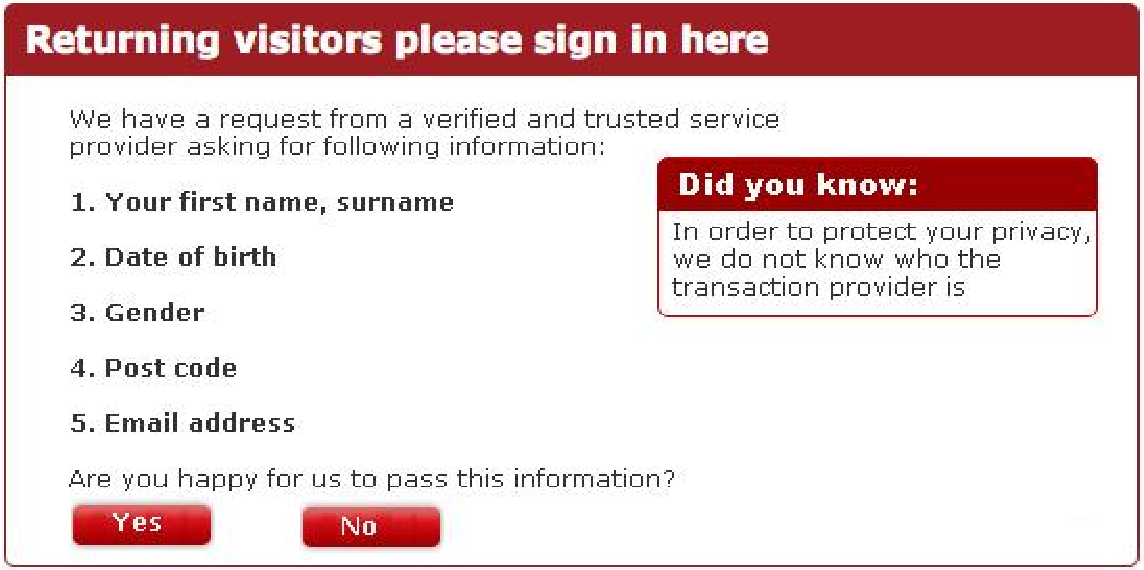
# 6. More externalities: all the stuff you put in place because passwords don’t work

- backup authentication questions I have to make up answers for – which I can’t remember later
- 2-factor authentication that doesn’t work when I don’t have cellphone reception (thanks, Google!)
- And no, I don’t want to be called by my friends in the middle of the night to vouch for them, so they can re-set their password (thanks, Facebook!)

# 7. They’d take Federated ID – if only they could understand it

- US and UK government – NSTIC program
- Usability issues:
  - You told me re-directs are suspicious!
  - Lack of feedback → forget to log out
- Trust issues: Users don’t understand
  - underlying commercial incentives
  - privacy protection mechanisms

POST OFFICE



## Returning visitors please sign in here

We have a request from a verified and trusted service provider asking for following information:

1. **Your first name, surname**
2. **Date of birth**
3. **Gender**
4. **Post code**
5. **Email address**

**Did you know:**

In order to protect your privacy, we do not know who the transaction provider is

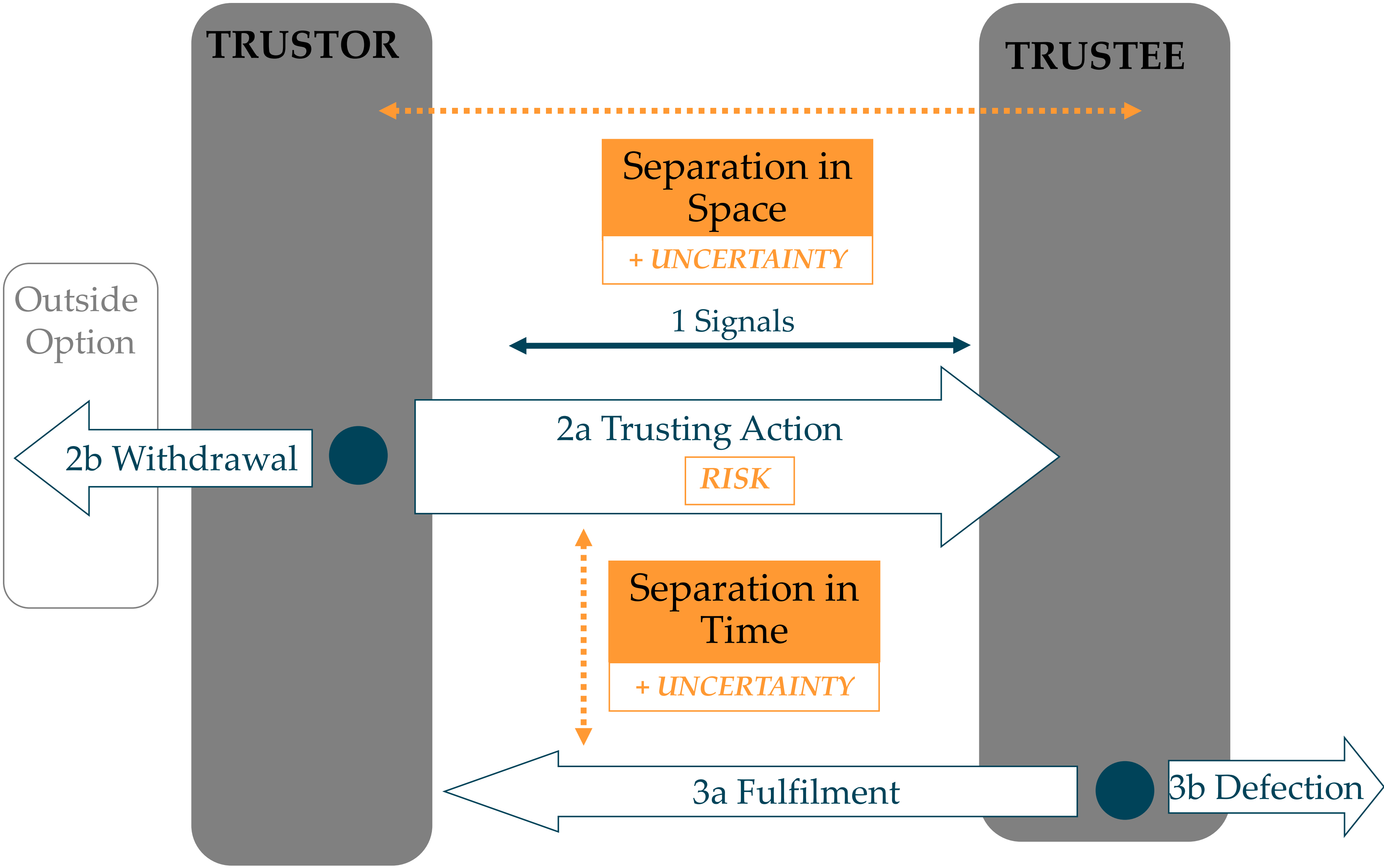
Are you happy for us to pass this information?

# Meanwhile, half a billion users trust …

- the 600 pound Gorilla, behaving badly?
- Facebook Connect – *“all the better to track you with”?*

# 8. They think they know better who to trust

- Trust signaling from the real world still informs trust decisions
- Split-second assessment of trust and motivation



TRUSTOR

TRUSTEE

Separation in Space

+ *UNCERTAINTY*

1 Signals

Outside Option

2b Withdrawal

2a Trusting Action

*RISK*

Separation in Time

+ *UNCERTAINTY*

3a Fulfilment

3b Defection

# Trust signaling problems

- Trust seals don’t work
  - Users won’t check/verify details – too time consuming
  - Misleading: suggest more protection than offered
- Social feedback is good – but reputation mechanisms too slow to prevent some attacks
- Perceived familiarity breeds complacency – Apple users beware …

# 9. They trust security architectures they shouldn’t

- Scary messages about non-threats
- Masking of actual risks – e.g. compromised CAs

# Trust Injection Attack - Results

- 143 participants completed the MTurk HIT
  - 128 passed the “check questions”
- 73% accepted the CA dialog (and thus made themselves vulnerable)
  - 77% believed that this increased their privacy protection
  - 21% believed there was no change
  - only 2% suspected that their privacy might be at risk
- Of those who clicked cancel
  - 64.7% believed it would not have effected their privacy
  - 29.4% believed it would have improve their privacy
  - only 5.9% thought it would have a negative effect.
- Usability
  - SUS usability score of 76.97 (out of 100)
- Complexity of SSL/CAs makes an excellent breeding ground for social engineering attacks.
  - This is a very easy and low risk attack to execute

# 10. They cling to myths

- *“I’m fine because …”* - beliefs in brands and service providers taking care of things
- ‘Trust halo’: Many app users attribute Appstore-type checking to Android apps
- Service providers take care of malware

# Conclusions

- Respect for users’ time and effort: it is valuable
- Complexity is the enemy:
  - Need clear simple guidance that works
  - Anytime. Anywhere. Mobile is only getting bigger.
  - And still allows users to get on with their activities
- Minimize disruptiveness of security: ‘smooth the path’ to secure behaviour

# Integration instead of obstacle security

- FCS Safeshop search: only display safe sites

https://www.solidauthentication.com/download/

# Attackers exploit human weaknesses

1. Distraction
2. Social Compliance
3. Herd behaviour
4. Dishonesty
5. Deception
6. Need and Greed
7. Time

Stajano & Wilson :
*Understanding scam victims: Seven principles for systems security*
CACM 2011

# … security designers should be on their side

- Focus on what users really can and should do
  - Minimize time and effort you require
  - don’t simply ‘pass the buck
  - Top target: authentication *“0 effort, 1 step, 2 factor”*
  - Usability researchers should help: task load and ‘fit’ metrics designers can consult
- Better risk communication
  - honesty, focus on consequences
- Maybe “Security measures that waste users’ time” should be in the OWASP Top 10?

# If government wants to transact online …

… it should make sure citizens can do so, securely

1. Can we make PKI work, please?
2. Provide authoritative advice, make safe configurations and tools available
3. ‘Road safety’ code with clear roles and responsibilities for users and service providers

# Questions?