Can We Make People Value IT security?

Wheeler Lecture 2017

M. Angela Sasse FREng

Professor of Human-Centred Technology

Director, UK Research Institute in Science of Cyber Security

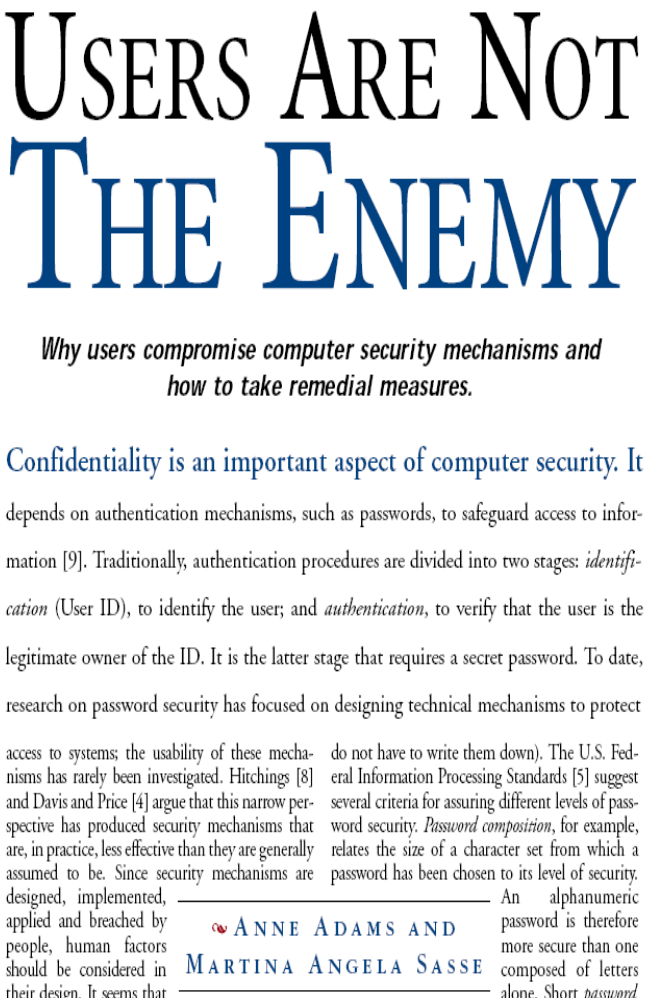
UCL

RISCS

Research Institute in Science of Cyber Security

Background

- Study on escalating cost of password resets in a company
  - Impossible workload (memory)
  - Induces workarounds (non-compliance)
  - Non-compliance → users disbelieve and disrespect 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

20 years on …

We know that:

1. Complex security causes mistakes
2. High workload security, disruption of and conflicts with primary tasks lead to non-compliance and *shadow security* practices
3. But still: many security measures have drain user time and effort for little discernable security benefits (e.g. ‘strong’ passwords, SSL warnings, CAPTCHAs)

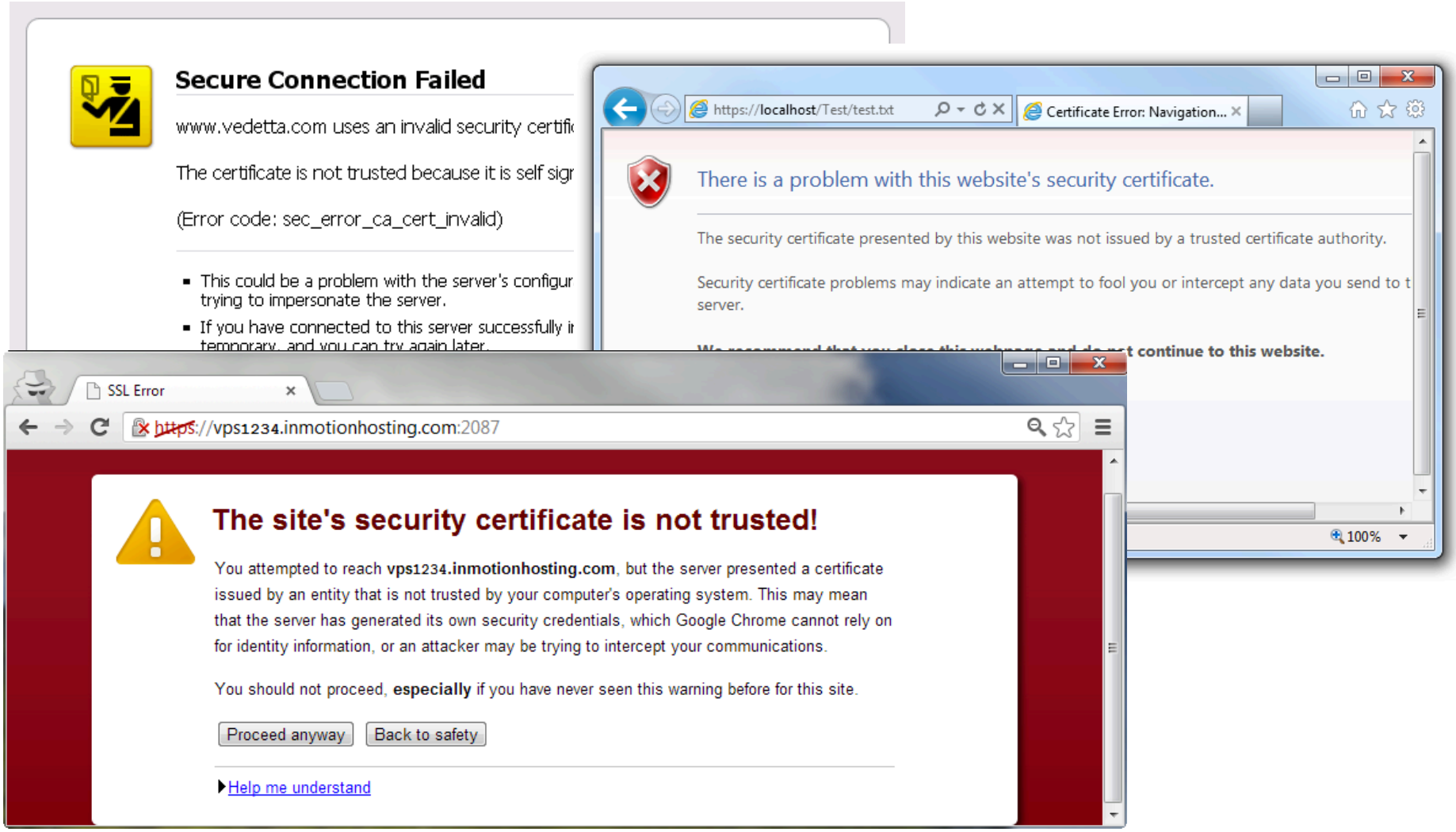
See also: C. Herley (2014) *More is not the Answer*. IEEE S&P Magazine.

Warnings

- Ignoring of a key usability principle – pop-up dialogue boxes should never be used for common events (Cooper 1995)
- Plus: high false positive rates, plus lack of visibility of consequences – has created habit of swatting and ignoring warnings

Krol et al. (2012): *Don't Work. Can't Work? Why it's time to rethink security warnings*

HTTPS Warnings



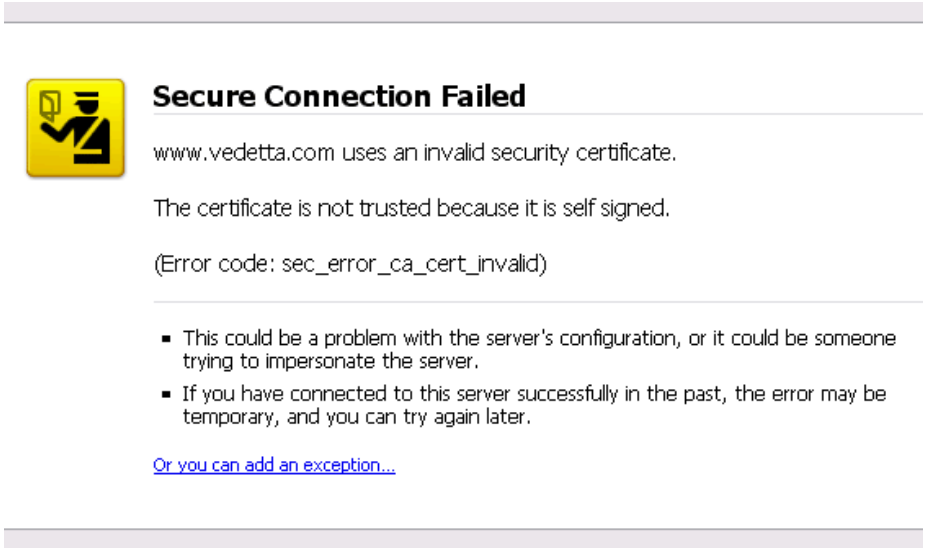
Wh

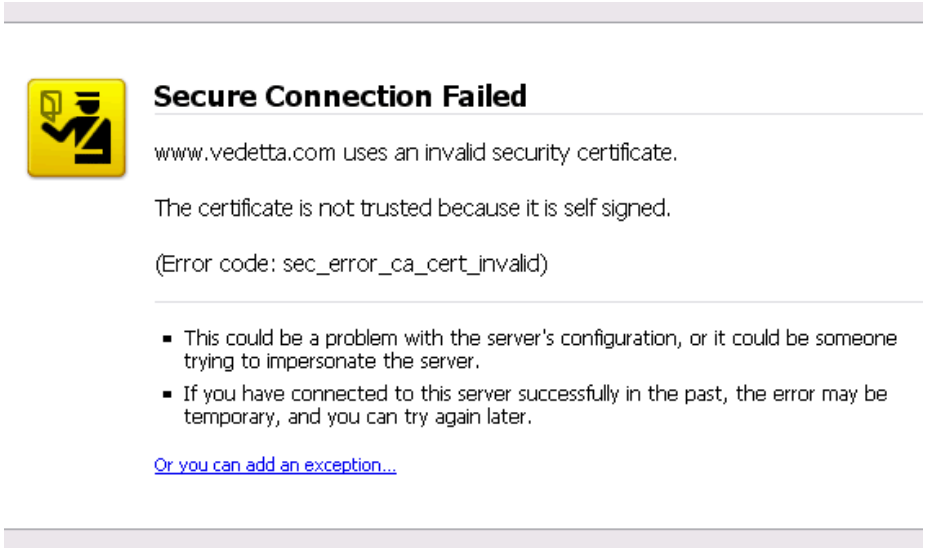
Adapted from Jonathan Nightingale

HTTPS: Administrator Mistakes

Akhawe et al. 2013: Server misconfigurations lead to

15.400 false positive per **1** true positive certificate warnings[1]





Trick …

- Felt at al. (2015) applied of recommendations from literature to Chrome SSL warnings
  - keep warnings *brief*
  - use *simple language* to describe *specific risk,* and
  - *illustrate* the potential consequences of going ahead
- Not much improvements
- Next ‘opinonated design’
  - to make it harder for participants to circumvent the warnings.
  - visual design to make the secure course of action look more attractive

… or treat?

- Anderson et al. (2015) putting users in fMRI scanner shows brain habituates
- Solution: change design (sizes, colour, text order so users cannot habituate – until 13th view of warning
- What next – electroshocks to force users to counteract habituation?

CAPTCHAs

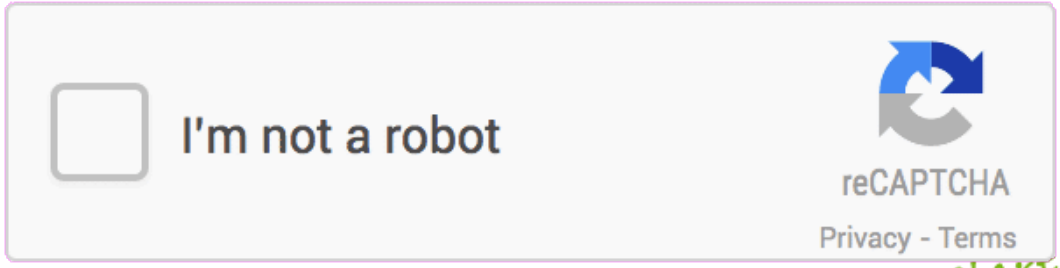
- Completely Automated Public Turing test to tell Computers and Humans Apart
- Type of challenge-response test to determine whether the user is human or a bot
- Application areas:
  - Free email account registration
  - Prevent automated guessing attacks
  - Prevent data mining/scraping
  - Prevent manipulation of online data gathering


RYANAIR.COM
Search » Select » Services » Payment » Itinerary
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
stop spam.
read books.
You do not have permission to access this website
if you are using an automated program
CONTINUE
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.

‘Usable’ CAPTCHAs?

- Make users jump through hoops to deal with attacks on service providers, not users themselves
  - *“Don't make users take responsibility for our problems.”* James Edwards

http://www.sitepoint.com/article/captcha-problems-alternatives/



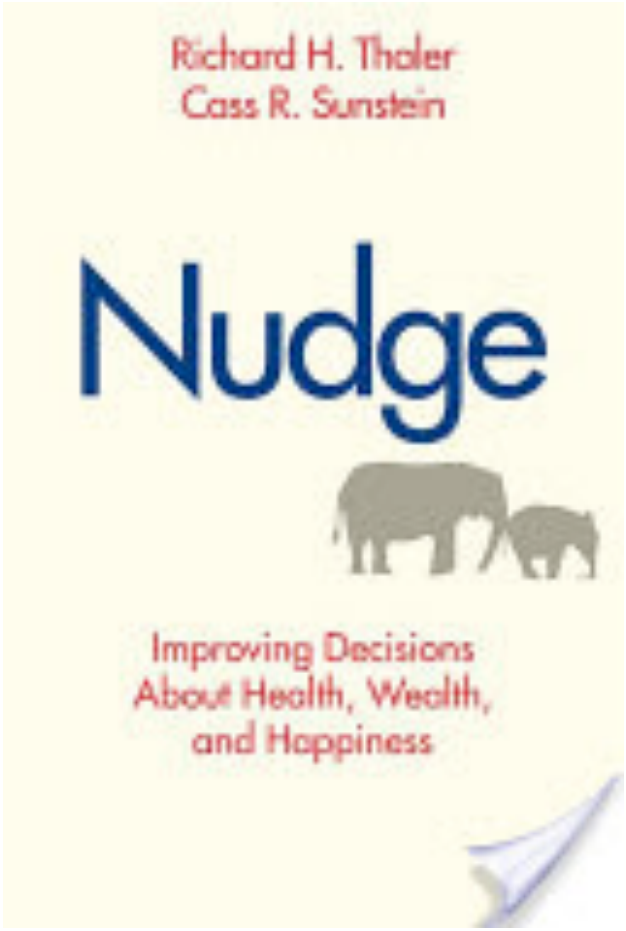
Click start to begin!

Am I Human?

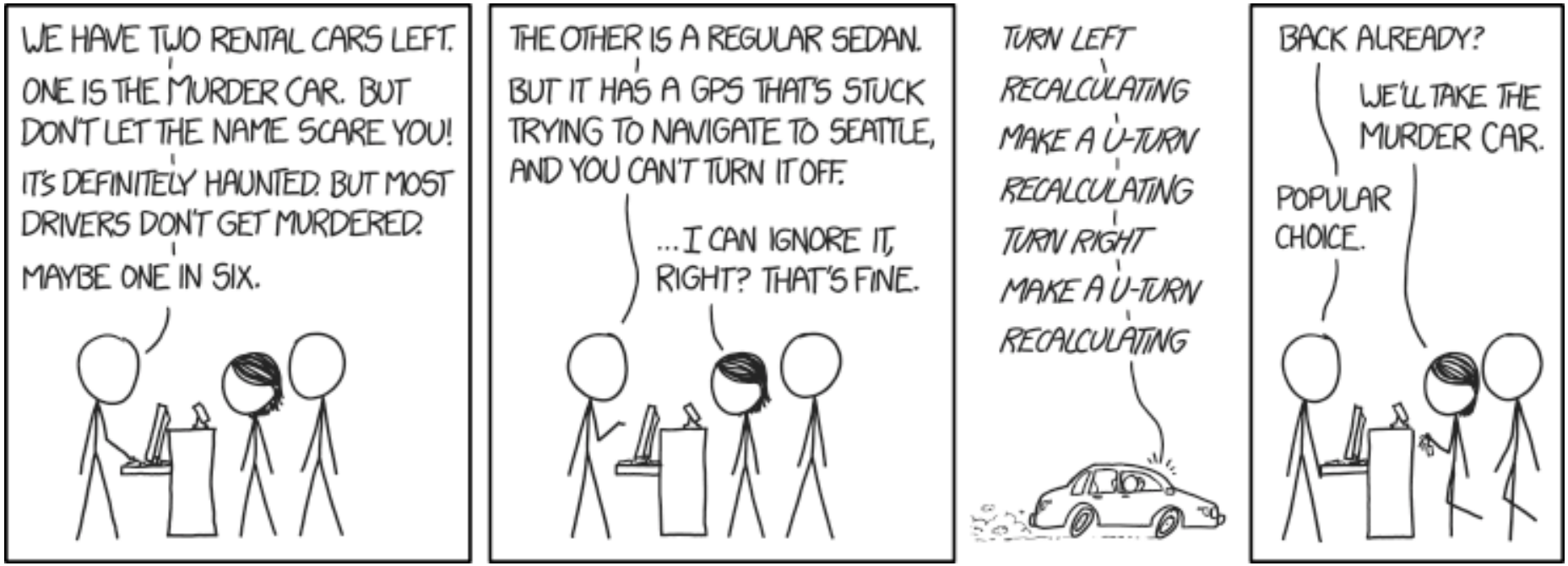
Check your humanity!

But there is nagging paternalism in security

- Often justified with ‘nudge’ behavioural economics
- Seen as a way of making people ‘do security’
- But: choices have to be genuine, and desirable



Many security propositions are like this …



XKCD https://xkcd.com/1837/

Re-birth of value-based design

The Denver Manifesto

WORKING DRAFT

We, the undersigned, recognize that values manifest themselves in every aspect of computing. Computing technologies and practices have become unavoidable cornerstones of most societies, including constituencies who may not be the direct users, developers, or designers of the technology. Values play key roles in the design, development and deployment of technologies, shaping and guiding what we imagine.

“It is important for these values to be explicitly and intentionally considered, not just with respect to the values intended but whose values are included, how conflicting values are negotiated, and how values are instantiated in deployed practice, especially but not solely when a technology is not fully transparent about how it produces its outputs.”

Meaningful consent

1. **Disclosure**: *provide accurate information about benefits and harms*
2. **Comprehension**: *the user must understand what is being disclosed*
3. **Voluntariness**: *user can reasonably resist participation*
4. **Competence**: *user has mental, emotional and physical competences to give informed consent*
5. **Agreement**: *clear opportunity to accept or decline*
6. **Minimal Distraction**: *user's attention should not be diverted from main task*

B. Friedmann, P. Lin & J. K. Miller: Informed Consent by Design
In Cranor & Garfinkel eds. Security and Usability 2005

Let's STOP the Biggest Lie on the web!

Stop! | Why? | How? | Action | About

Confess and protest against the Biggest Lie!

☑ I have ***not*** read the Terms & Conditions many times but often agree to them anyway.

There must be a better way!

I confess - and protest! *

* No personal information collected. We just count.

Doc Searls blogged about BiggestLie.com:

“We lie every time we "accept" terms that we haven’t read ... We need to change that.”

People do value privacy

Contrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests. Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages—between 73% and 86%--say they would not want such advertising.

Turow et al. (2015): Electronic copy available at: http://ssrn.com/abstract=1478214

“Why Johnny Can’t Encrypt”

- Whitten & Tygar (1999) Graphical UI to PGP 5.0
- Only 2/12 participants managed to complete task of generating keys, sending encrypted and decrypting received messages; some who sent plain text thought they had encrypted them!

Solution?

- Alma Whitten created the LIME tutorial to educate users about public key cryptography

"There are significant benefits to supporting users in developing a certain base level in generalizable security knowledge. A user who knows that, regardless of what application is in use, one kind of tool protects the privacy of transmission, a second kind protects the integrity of transmission, and a third kind protects the access to local resources, is much more empowered than one who must start afresh with each application."

www.gaudior.net/**alma**/MakingSecurityUsable.pdf

A telling observation …

"… when presented with a software programme incorporating visible public key cryptography, users often complained during the first 10-15 minutes of the testing that they would expect 'that sort of thing' *to be handled invisibly. As their exposure to the software continued and their understanding of the security mechanism grew, they generally ceased to make that complaint."*

Clear expression of what users (don't) want –
Overruled by well-meaning paternalism

“People want to protect themselves, not join a crypto-cult.”

Philip Hallam-Baker at PKI Workshop 2006

Encrypted tools today

Ruba Abu-Salma (UCL) interviewed 60 users of chat – all had tried to use encrypted chat tools, but most stopped using them

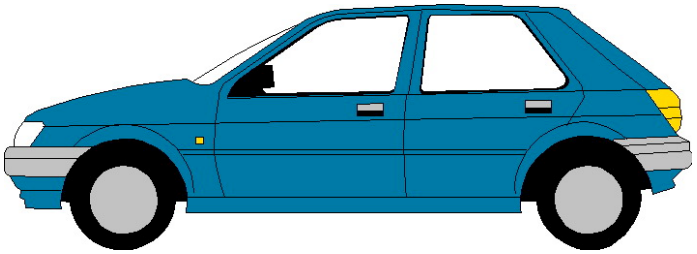
1. Lack of utility
2. Usability problems
3. Misconceptions - about risks, and protection offered by the tools

R Abu-Salma paper at IEEE S&P this week!

Utility

1. Primary task = communication = need to be able to reach your intended communication partner
2. Or partners – secure tools don't support group chat

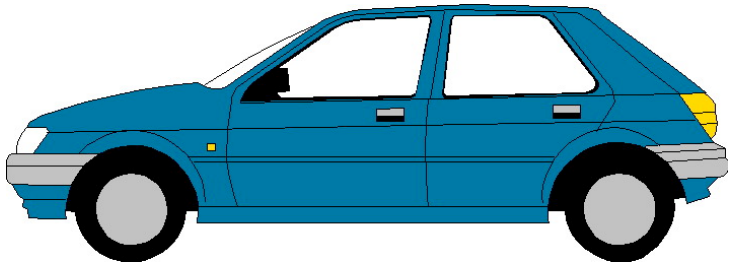
if the chat tool was a car …



Usability

1. Many tools have installation problems
2. Key exchange is cumbersome
3. Some are slow to decrypt (e.g. *Threema*)

If the chat tool was a car …



Another Example: Desktop Sandboxing

App sandboxes isolate apps from each other and constrain them, to limit the spread of malware.

Sandboxes were built with prescriptive assumptions about how users organise their data. They:

- Reduce functionality by forcing app developers to drop features and plugins
- Force users to organise their files in specific, inconvenient ways

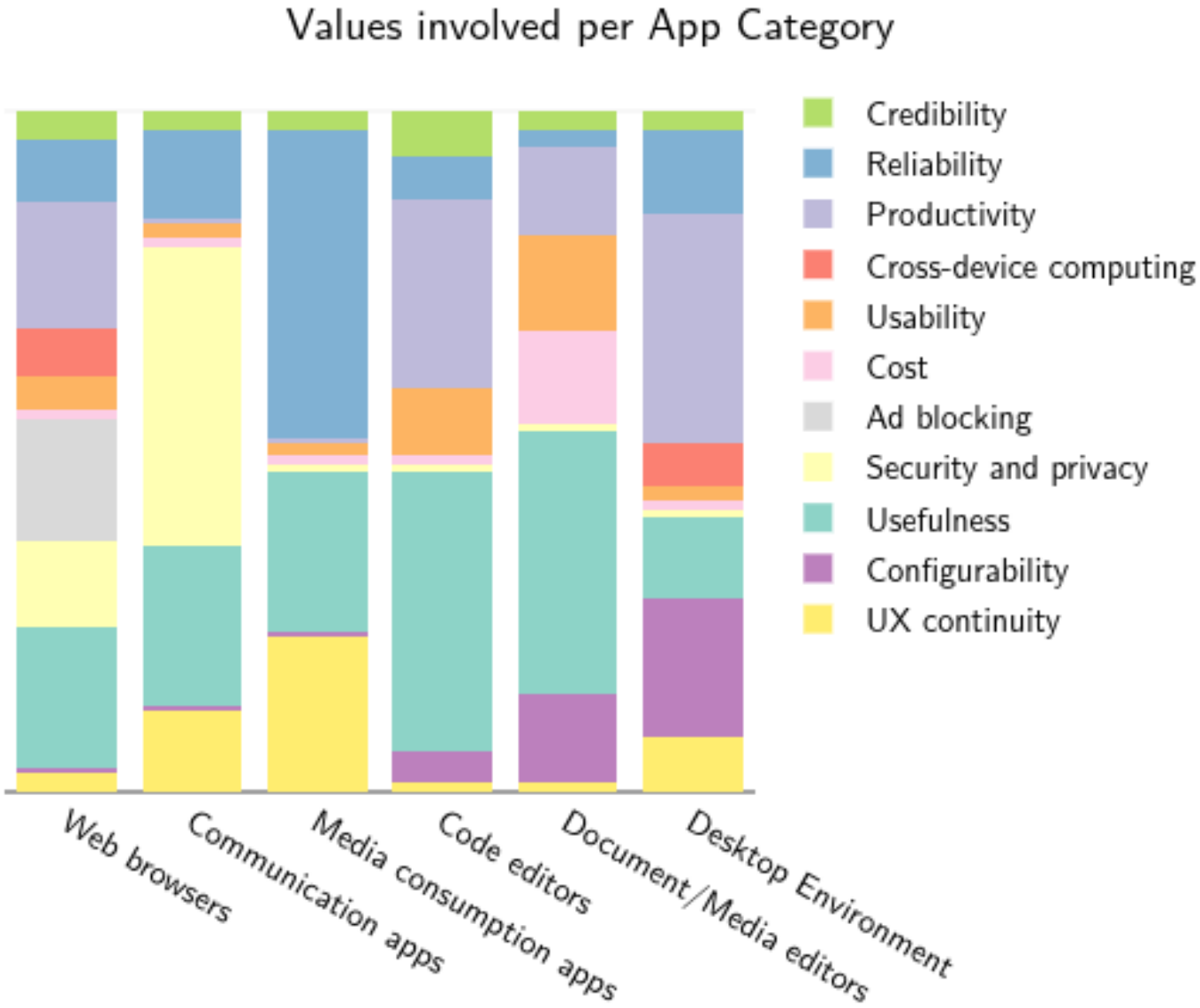
Sandboxes vs. App Features

Interviews w/ 13 users (med. 1:14 hour, 140 statements per interview). Analysed values involved in app adoption/abandonment/adaptation decisions.

- Users value usefulness the most. Sandboxes conflict with that by removing features and plugins
- Users don't value security much. Half would reject a security update that removes a feature they use
- Unsurprisingly, developers don't want sandboxing

S. Dodier-Lazaro et al.: No Good Reason to Remove Features: Expert Users Value Useful Apps over Secure Ones. *Procs HCII 2017.*

Sandboxes vs App Features

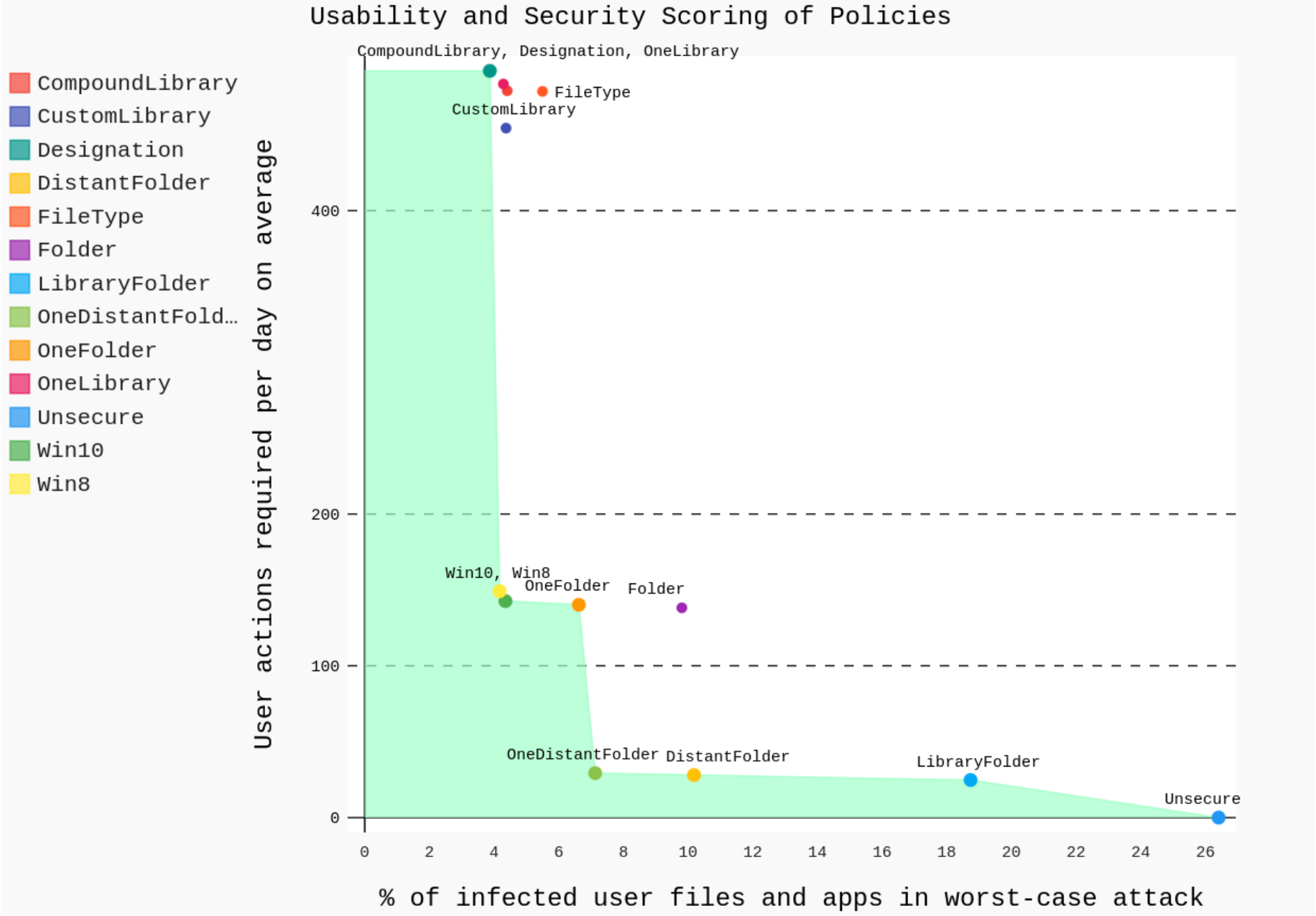


Is sandboxing worth the price?

First ever usability and security evaluation of AC models for sandboxes show additional issues.

- Reduces functionality because data cannot be moved to where it is needed
- Does not support keeping different projects / client's data (or work / life data) separated
- Common sense dictates we deploy sandboxes only if they provide more benefits than costs!

S. Dodier-Lazaro et al.: Comparing the Usability and Security of Desktop Sandboxes' File Access Policies. *To be published.*

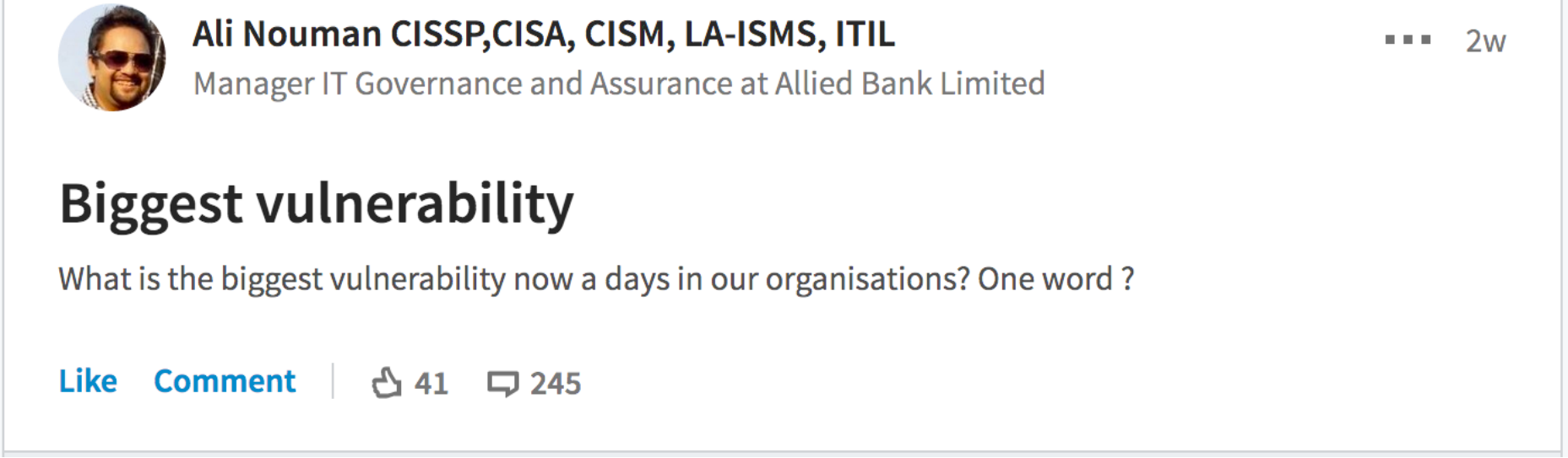

Usability and Security Scoring of Policies
CompoundLibrary
CustomLibrary
Designation
DistantFolder
FileType
Folder
LibraryFolder
OneDistantFold…
OneFolder
OneLibrary
Unsecure
Win10
Win8
User actions required per day on average
CompoundLibrary, Designation, OneLibrary
FileType
CustomLibrary
Win10, Win8
OneFolder
Folder
OneDistantFolder
DistantFolder
LibraryFolder
Unsecure
400
200
100
0
0 2 4 6 8 10 12 14 16 18 20 22 24 26
% of infected user files and apps in worst-case attack

Security is often less than benign paternalism …

"Not only in security is it the case that an ordinary person has a problem and a friendly mathematician solves a neighbouring problem. An example that is of interest here is the electronic book. We have a pretty good idea of the semantics of the paper book. We go and buy it, we can lend it to our spouse or to a friend, we can sell it, we can legitimately copy small bits of it for our own use, and so on."

R. Needham: Computer security? The Clifford Paterson Lecture, 2002. http://rsta.royalsocietypublishing.org/

And experts bond by demonising users who don't do obey …



Ali Nouman CISSP,CISA, CISM, LA-ISMS, ITIL
Manager IT Governance and Assurance at Allied Bank Limited

··· 2w

Biggest vulnerability

What is the biggest vulnerability now a days in our organisations? One word ?

Like Comment | 41 245

Swaminathan Sangaran People

Like ··· 4d

Shahjahan Khan Employee

Like ··· 4d

Tridep Lal As far my experience in auditing I feel Careless people , Disgruntled Employees [privilege exploitation], Improper Systems and device configuration and BYOD

Like ··· 4d

TP TSHERING PHUNTSHO homo sapiens?

Like ··· 4d

Daniel Okoturo Lack of company awareness and People

Like ··· 4d

René Stadhouders The human factor

Like ··· 4d

Gusztav Krekity Humans the weakest link

M. Angela Sasse FREng Bad_tech

··· 4d

M. Angela Sasse FREng Unworkable_policies

··· 4d

M. Angela Sasse FREng
Security_specialists_who_just_blame_people_who_can't_cope_with_the_above

··· 4d

Jermund Ottermo If technology isn't making your life easier, you're doing it wrong... :D Don't blame the fool, blame the not foolproof system.

Unlike | You

··· 4d

Dariusz Synowiec Boss who don't want to spend money on staff training

Like

··· 4d

M. Angela Sasse FREng 'Training' is not the answer to bad tech+unworkable policies - you can help people understand and learn 'how-to' - but only if what you are asking for is achievable in real work+life situations. Stop demonisation and blaming of users - next week at CyberUK the NCSC is running a 'People are the strongest link' session.

··· 4d

Winston M. GREM, GCIA, CHFI Human error ;)

Like ··· 3d

Margaret H Brennan, MSc Is and always has been... ... Users

Like ··· 3d

Premysl Blahut People

Like ··· 3d

Drew Lewis Users

Like ··· 3d

Ian Trump, CD, CEH Humans

Like ··· 3d

Neil Cattermull Staff

People/Employees/Humans	90%
Stupidity	5% Stupidity (by humans)
insiders	7
Leadership/Management	7
Attacks	5
Technology	5
Vendors	2
Governance	2
Policy+process	1

"It's us" – 6 - but not only 3 clearly say – us, security people.

Back to the Denver Manifesto …

"As a long-term strategy to improve practices in industry and academia, we believe educational programs in computer science and adjacent fields should include focused attention to the values intertwined with the other aspects of career preparation for the field. This training should provide students with the tools necessary for discussing and evaluating relevant values and tensions between them. In addition to providing tools for assessing and communicating about direct impacts, this education should foster an understanding of indirect externalities and risk evaluation, without equating risks with harms."

“It should prepare students to think critically, reflectively, and empathetically. It should prepare students to integrate diverse perspectives, and understand the cultural and historical contexts that shape present conditions. It should provide students with an understanding of how responsibility for creating products and systems that instantiate values may be distributed. It is a moral imperative for upstanding individuals in this field not to abdicate responsibility for the values manifest in the products of their work, or those espoused in their work environment.”

Or, as Jean-Luc would put it:

Slides 41-44 have been removed for reasons of confidentiality

The need for engagement with staff and citizen-clients

- real-world security problems are complex, need interaction to tease apart
- *"the term 'security' is not a useful concept– it is more normal to speak of certainty within a shared/ desired characteristic is achieved."*
  - Real-world security research requires an understanding of what is of *value* to a particular community
  - Behaviour change takes time. "*It doesn't happen very quickly*"
  - Often, underlying cause is out-dated and/or badly configured IT – more of this shortly

And we have just seen the security implications of that …

- ‘security awareness’ that doesn’t help

“We urge you to be vigilant and not to open emails that are unexpected, unusual or suspicious in any way. If you experience any unusual computer behaviour, especially any warning messages, please contact your IT support immediately and do not use your computer further until advised to do so.”

UCL IT Department

Security

63

Police anti-ransomware warning is hotlinked to 'ransomware.pdf'

This (probably) isn't a spear phishing attack but we were too afraid to verify

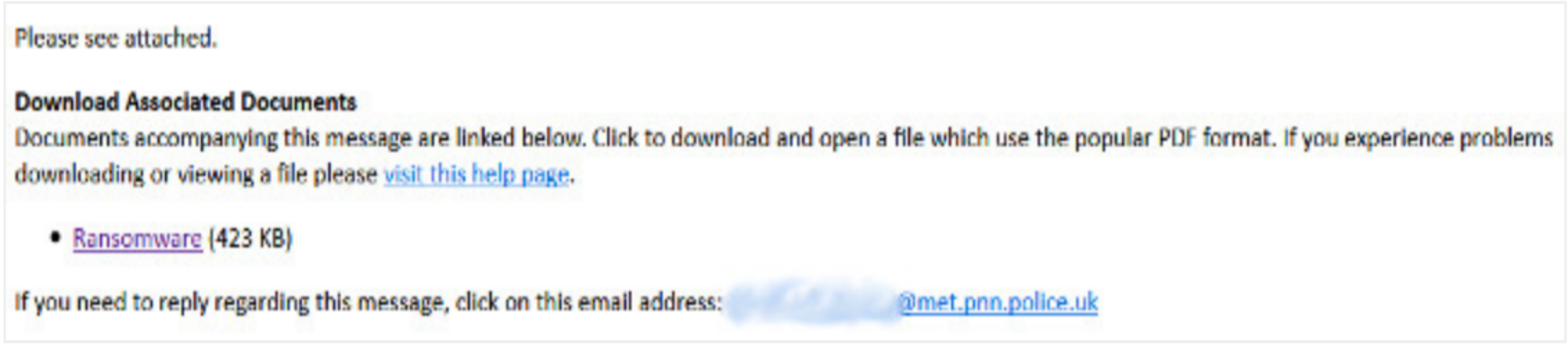
17 May 2017 at 12:40, Gareth Corfield

Official anti-ransomware advice issued by UK police to businesses can only be read by clicking on a link titled "Ransomware" which leads direct to a file helpfully named "Ransomware.pdf".

In case you've been living under a rock, large chunks of the digitised world, including most of the NHS, were, ahem, *digitally disrupted* by the WannaCrypt ransomware last week.

"Following the ransomware cyber attack on Friday 12 May which affected the NHS and is believed to have affected other organisations globally, the City of London Police's National Fraud Intelligence Bureau has issued an alert urging both individuals and businesses to follow protection advice immediately and in the coming days," it said. Standard stuff.

This followed:



Please see attached.

Download Associated Documents

Documents accompanying this message are linked below. Click to download and open a file which use the popular PDF format. If you experience problems downloading or viewing a file please visit this help page.

- Ransomware (423 KB)

If you need to reply regarding this message, click on this email address: [redacted]@met.pnn.police.uk

As you can see, we clicked the link – and after routing through some standard email marketing click tracker stuff, it hotlinks to a file titled "Ransomware.pdf". We chose not to let it open in our VM.

People really value trustworthy expert advice

- *Cacophony of 'advice from different sources unhelpful*
- people assess trustworthiness in terms of *competence* and *motivation*
  - undignified squabbling over who is to blame name-calling

  doesn't signal either
- lesson to be learnt for future major incidents!

Improving security by investing in other things …

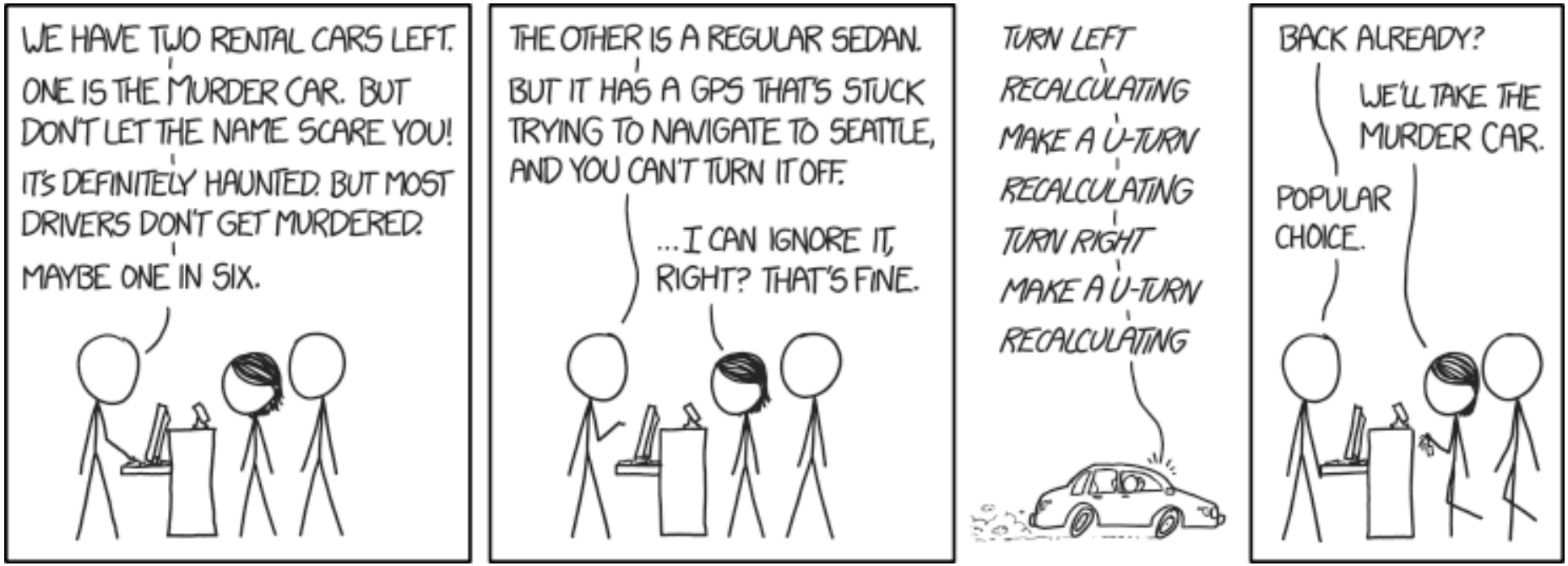
- Sometimes, investing in other aspects can improve security:
- People: proper staffing levels (stress and fatigue make employees vulnerable)
- Environment: lighting, ventilation, PA systems that work – see Harvey Molotch research on NY pub transport
- Improve overall resilience, rather than just defend against specific threats

Molotch (2014): Everyday Security: Default to Decency.
IEEE Security & Privacy Magazine, Issue 6, Nov.-Dec. 2013, pp. 84-87

Conclusions

1. Categorial imperative of human-centred security: don’t waste people’s time and attention
2. Security paternalism is unhelpful even when it is benign – and often used to mask incompetence, vested interests, unwillingness to change
3. Instead: understand user activities and values, and support them
4. Security people need mind- and language shift, and additional skills to engage and change.

Questions?


WE HAVE TWO RENTAL CARS LEFT.
ONE IS THE MURDER CAR. BUT DON'T LET THE NAME SCARE YOU!
IT'S DEFINITELY HAUNTED. BUT MOST DRIVERS DON'T GET MURDERED.
MAYBE ONE IN SIX.
THE OTHER IS A REGULAR SEDAN.
BUT IT HAS A GPS THAT'S STUCK TRYING TO NAVIGATE TO SEATTLE, AND YOU CAN'T TURN IT OFF.
...I CAN IGNORE IT, RIGHT? THAT'S FINE.
TURN LEFT
RECALCULATING
MAKE A U-TURN
RECALCULATING
TURN RIGHT
MAKE A U-TURN
RECALCULATING
BACK ALREADY?
POPULAR CHOICE.
WE'LL TAKE THE MURDER CAR.