Security Behaviours

COMS30038 Lecture 6 - Usable Security

Dr Ramokapane

University of BRISTOL

Bristol Cyber Security Group

Humans-in-the-Loop Recap

HiL is where the **human** is **expected** - in some way - **to reason** about the world **to make** a **system influencing decision**.

But humans are limited by their **capacity**, **subject knowledge** & **motivation**. Sometimes they just get things wrong.

usable security (part a)

credit: olly (fotolia)

The Cyber Security Body of Knowledge

A comprehensive Body of Knowledge to **inform and underpin education and professional training for the cyber security sector**.

The CyBOK project aims to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts to form a Cyber Security Body of Knowledge that will provide much-needed foundations for this emerging topic.

The project, funded by the National Cyber Security Programme, is led by the University of Bristol's Professor Awais Rashid, along with other leading cyber security experts - including Professor Andrew Martin, Professor Steve Schneider, Professor Emil Lupu and Dr Howard Chivers.

CyBOK

Some Stats

CyBOK covers 19 knowledge areas grouped as:

- Human, Organisation & Regulatory Aspects
- Attacks & Defences
- Systems Security
- Software & Platform Security
- Infrastructure Security

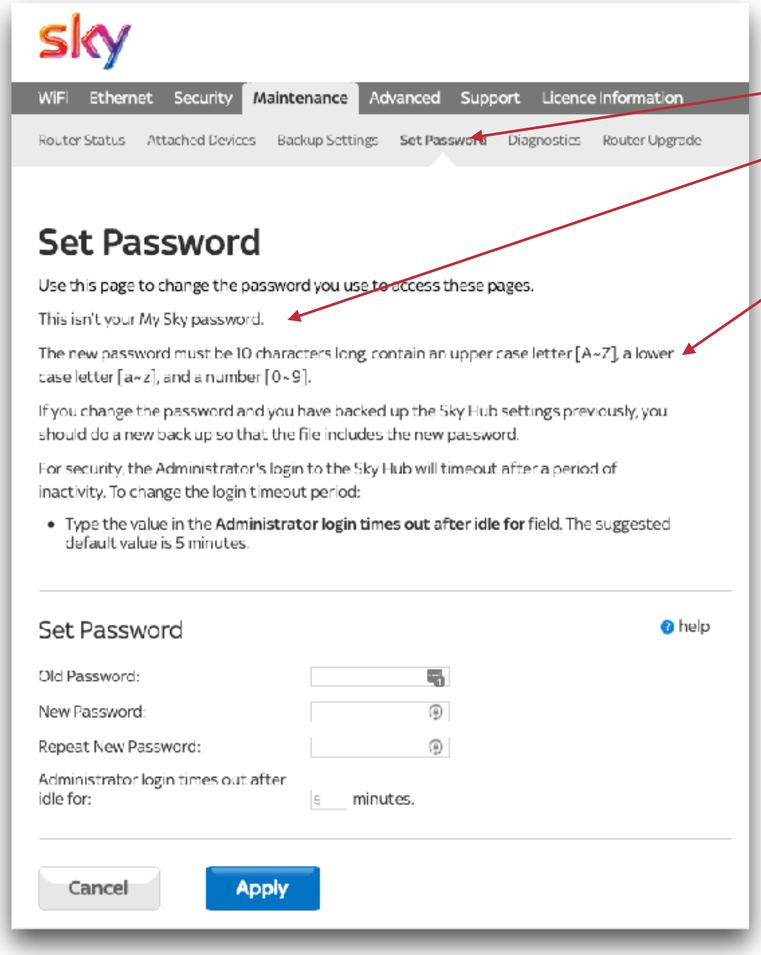
110 Expert authors, reviewers and advisors
828 Pages long
1,839 Authoritative sources

The COMS30038 Security Behaviours unit borrows heavily from several knowledge areas and especially so from “Human Factors”
https://www.cybok.org/media/downloads/Human_Factors_issue_1.0.pdf

“it [security] must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.”

Kerckhoffs 1883

So why do we still have…



buried in menu structure rather than enforced on setup

nothing to enforce differences

outdated structure guidance

Will the user know to go digging for a password change dialogue or should they be modally forced at setup?

Is 10 characters enough, today? It's 2^{53} attempts to brute force. In 2018 a PC with GPU took 9 hours!

How about today?

Useful Stuff

NCSC. Three Random Words
https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

NIST. Usability Considerations - Digital Identity Guidelines SP800-63b
https://pages.nist.gov/800-63-3/sp800-63b.html

Wikipedia (yup I went there). Password strength.
https://en.wikipedia.org/wiki/Password_strength

Longer more complex passwords!

True. We could add in symbols and get a bump to 65.5bits (23 days c.2018)

We could make the password longer, say 15 characters in length (464M years)

BUT

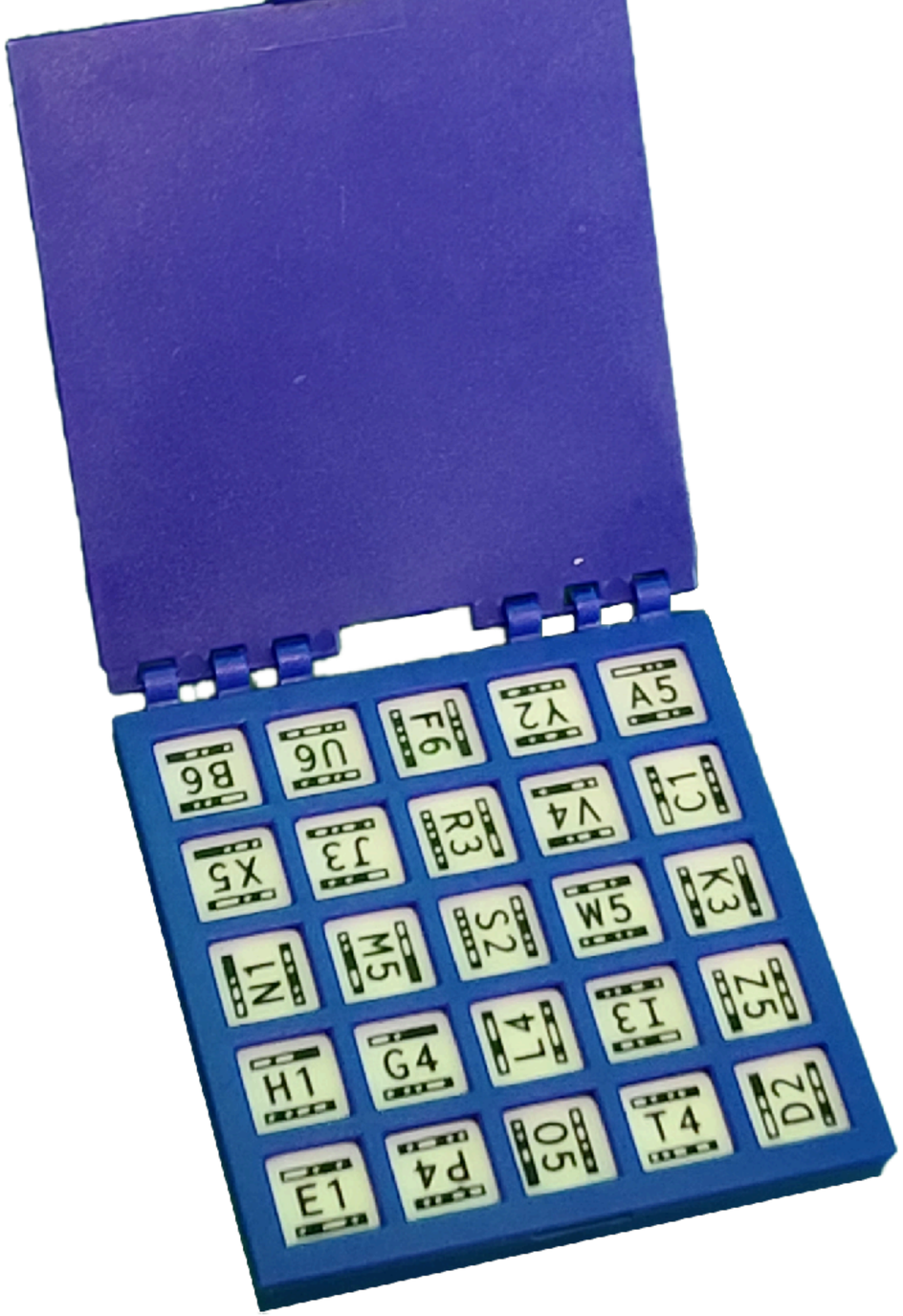
Can you remember 15 random characters for every site? We're back to human capacity issues and their workarounds.

The problem is…

We are trying to fit the human to the task!

rather than

FITTING the TASK to the HUMAN



Open and tangible

Our open software for reading `DiceKeys` and performing cryptographic operations with them is available for you to inspect, compile, modify, and use for eternity.
In contrast to hardware designed to resist inspection, you can inspect every aspect of `DiceKeys` with your own eyes. Your security is literally in your own hands.

Designed to last a human lifetime

Most products are designed to be replaced, and many technology products are designed to be replaced dozens of times over a human lifetime. In contrast, one need only open up a decades-old game to observe the longevity of dice.

Future-proof

In 50 years, our devices may no longer support Bluetooth or USB-C, but we will still have eyes and our devices will still have cameras. Even if the company behind `DiceKeys` is long gone, our license gives you access to use our software for eternity, and allows the open-source community to maintain and improve it.

So yes DiceKeys (just as an example) may create > 196bits keys but:

- Have you ever to keep ALL the pieces in a game box intact?
- What happens if the box breaks or pops open?
- Will the plastic or ink degrade over a person's lifetime making them unreadable?

Maybe it's usable now, maybe not. Will it always be usable?

<u>Is this just another case of fitting the human to the task?</u>

Steps forward for usable security…

DASHLANE

LastPass •••|

1Password

With the odd really huge leap backwards!

```
<input type="text" onselectstart="return false"
                   onpaste="return false;"
                   onCopy="return false"
                   onCut="return false"
                   onDrag="return false"
                   onDrop="return false"
                   autocomplete=off
/>
```

! Foundational Reading !

This is a seminal work - so read it! Sasse & Flechais made the direct link between between human factors (HF/E) knowledge from the safety aware sectors and their understanding that people are fallible with security tasks as well.

They take HF/E learnings and set out that, as with physical systems, **for security to work and be effective it has to be usable**.

The work also sets out the relationship between organisations (comprising of people) and their culture, creating a socio-technical system within which there are both technical and human aspects.

Useful Stuff

Sasse, M.A and Flechais, I. 2005 Usable Security - Why do we need it? How do we get it? https://discovery.ucl.ac.uk/20345/2/cransimpsonbook.pdf

Note: Early works exist but this paper brings concepts together nicely.

Roots of Usability in Security

Saltzer & Schroeder's 1975 paper established ten principles for designing in security, three being rooted in behavioural science:

1. **Psychology**: the security mechanism must be 'psychologically **acceptable**' to the humans who have to apply it

2. **Human Factors and Economics**: each individual user, and the organisation as a whole, should have to deal with as **few distinct security mechanisms as possible**

3. **Crime Science and Economics**: the **effort required** to beat a security measure should **exceed** the resources and potential **rewards** for the attacker

Half of Kerckhoffs 1883 principles for secure communication were "it must be **easy to use** and must neither require **stress of mind** nor the **knowledge** of a long series of rules"

Remembering back to HiL that **Humans have limited capacity** and sometimes **just don't know what to do.**

CyBOK

Usability out front and centre

The International Standard ISO 9251-11:2018 defines usability as:

“The effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments.”

The UK’s National Cyber Security Centre has a whole stream of work on people-centred security which looks to how security works for people - and not the other way around.

As such security tools need to be assessed for usability based on:

- **Effectiveness** **"Can users achieve their goals?”**
- **Efficiency** **"What resources are expended to do so?”**
- **Satisfaction** **"What is the user level of comfort and acceptability?"**

But even today in 2022, there is **no formal definition** of what Usable Security is, and we rather tend to look to the intersection between Usability and Cyber Security.

Useful Stuff

NCSC. 2017. The way to make security that works is to make security that works for people. https://www.ncsc.gov.uk/information/people-strongest-link

Fitting a task TO the human

1 **User capability** “There are general capabilities and limitations – physical and mental – that apply to most humans. Giving humans a task that exceeds their capabilities means we set them up to fail.”

2 **User goals & tasks** “Human behaviour is essentially goal-driven. People perform tasks to achieve goals… designing the technology tools so people can complete these tasks effectively and efficiently is the most fundamental aspect of usability.”

3 **Physical & social contexts of use** “Both the physical surroundings and the social environment in which people have to perform security tasks affect performance and security.”

4 **Device capability** “the physical characteristics of a device may make interaction with security mechanisms difficult in certain circumstances. Some characteristics of the device can result in security mechanisms becoming difficult to use in any circumstance.”

CyBOK

usable security (part b)

credit: olly (fotolia)

1 - User Capability (& Limitation)

We will cover bias as a separate lecture as it is such a large and important topic but for now when considering physical and mental aspects the key takeaway is **giving a human a task which exceeds their capability essentially sets them up to fail.**

Humans are really **synchronous** - it's hard to near impossible to do multiple things at the same time (try patting head and rubbing stomach - it requires a lot of mental concentration).

And this can be particularly acute with things like recognising security signals - both masked (phishing) and deliberate (status indicators from devices). It can lead to alert fatigue.

lgeorge25 "Tree of life" - pt with LVAD, septic, on pressors and CRRT

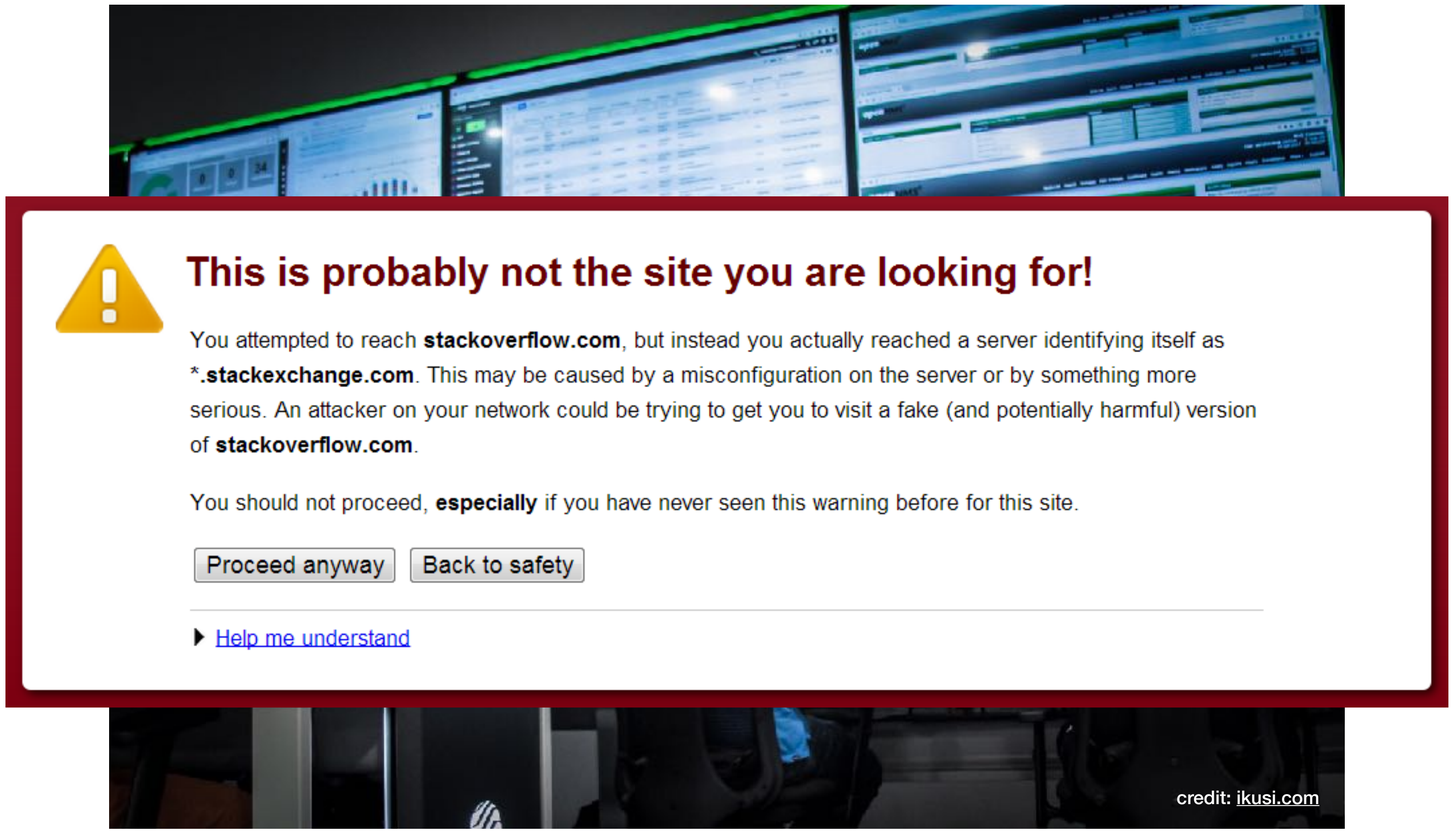
Alarm fatigue can be very real

Imagine sitting in a security operations centre, monitoring dozens of screens and hundreds of different measures to keep an eye out for alerts.

There are plenty of false positive alerts that for the human to filter out is a very high cognitive load, so eventually we almost become blind to those we see frequently.

This is one area where a lot of work has gone into better filtering through techniques like machine learning.

BUT alarm fatigue can hit us all…



Useful Stuff

Buczak, A. & Guven, E. 2015 A Survey of Data mining and machine learning methods for cyber security
https://ieeexplore.ieee.org/abstract/document/7307098

Pietraszek, T. 2004
Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection
https://link.springer.com/chapter/10.1007/978-3-540-30143-1_6

The challenge of mental encoding

Another key aspect of capability is the crucial difference between short and long term memory. You need to mull on things in short term memory to code to long term memory - it's a repetitive thing.

Remember when you had to recall your student ID and how for the first few times you needed to look it up?? What about your student number or email address?

It’s all xx###### or ######## or xx######@bristol.ac.uk or is it name@bristol.ac.uk?

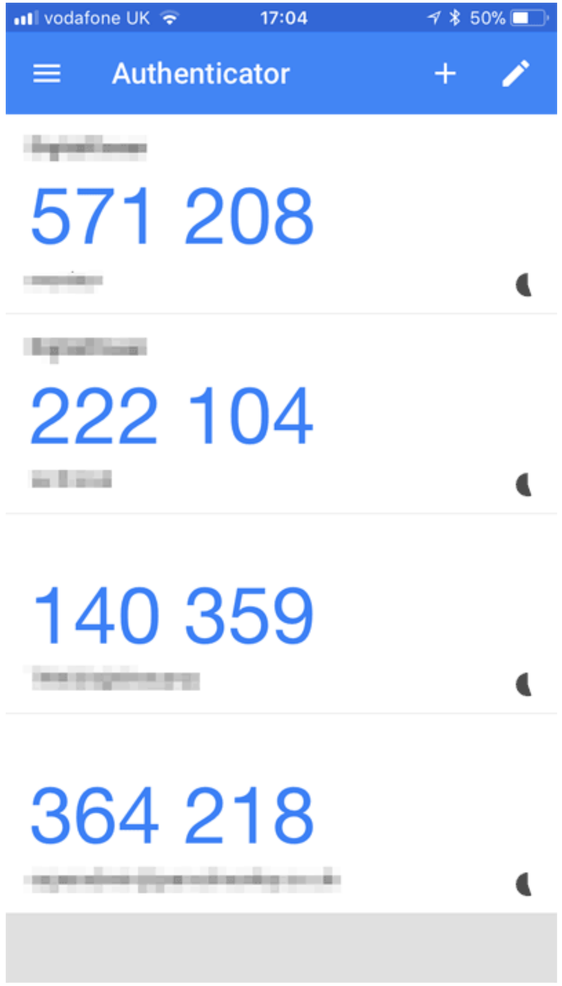
This leads into biases, and how we access memory - but that's for another day.

Short term and long term memory

Passwords are a great example of where STM and LTM are at play.

Most will have used a one-time-passcode, possibly one of those provided by an authenticator app. You only remember it for as long as is needed to use it once. No point encoding it in memory as 60 seconds later it is invalid.

BUT as with those StudentIDs, think of passwords you regularly use, and if you are super sensible and use a password wallet for extra specially long and complex passwords - the master key for that wallet. It is well encoded to LTM as without it.... :/

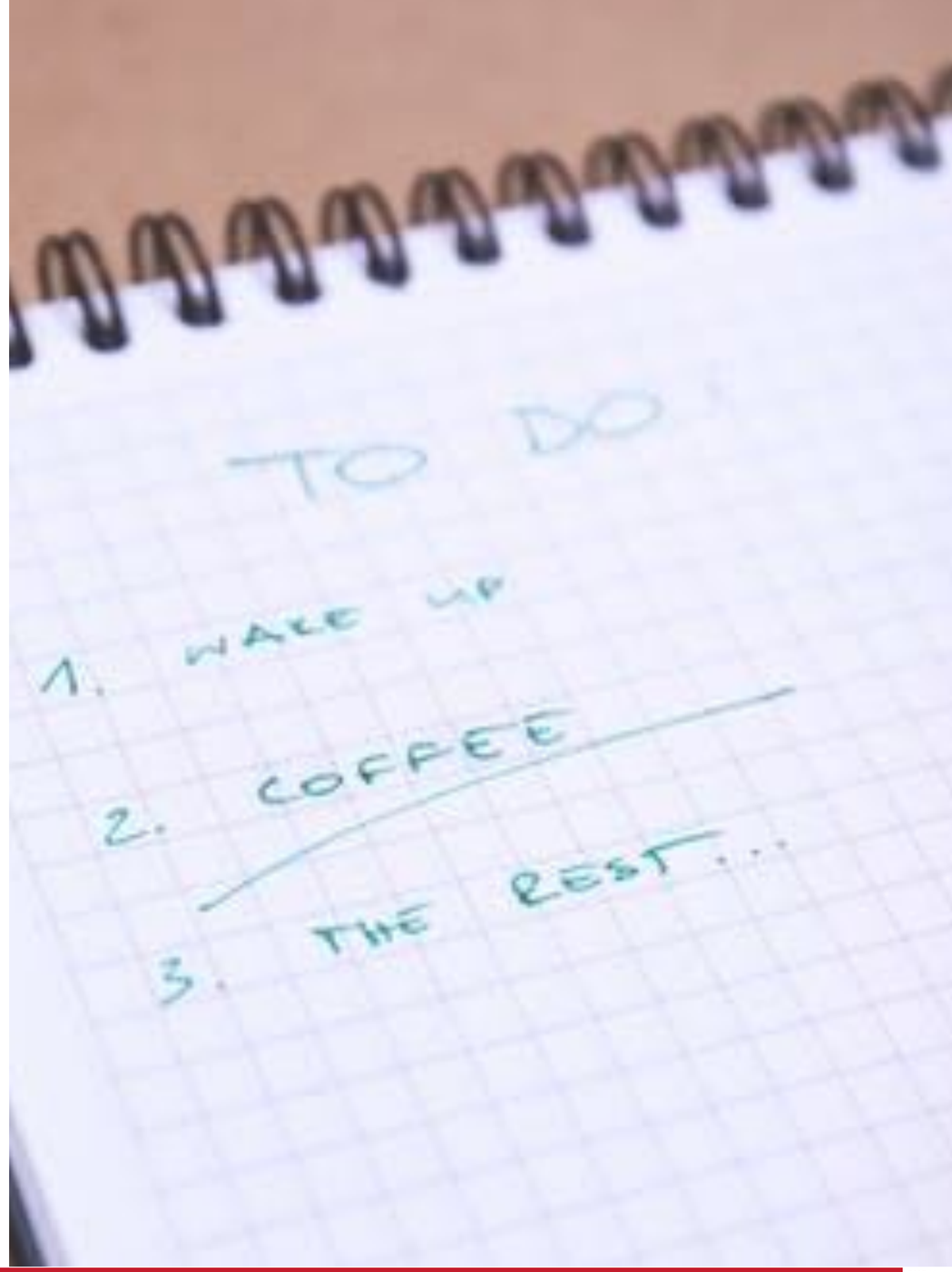


2 - Goals and Tasks

Human behaviour is goal-driven, and we tend to split goals into tasks which we work through (synchronously). These are our “production” tasks, the things we are looking to accomplish, **the job**.

But they are supported by “enabling” tasks which are the things we need to do to be able to undertake those “production” tasks - the infrastructure if you will. Unless you are building or operating security tools, then cyber security would normally be considered, enabling.

So it is a secondary task, that can allow for work to happen, but can also get in the way. And as such humans can view security as counter-productive to a key work task, and be reluctant to undertake it, or even find workarounds for it.



Workarounds are why we fit the task to the human

Employees when asked to focus on production tasks, and are rewarded thusly, impacts negatively on security compliance. The enabling task is driven so far back that it just isn't considered in pursuit of the work. Just like pretty much every Privacy T&Cs, or GDPR cookie you just click to get to the website or app you were seeking.

So to avoid those workarounds for security we must make then primary (production) tasks.

How does this fit with human in the loop and can you see the challenge between production & enabling tasks in the HiL example for the spread of Mirai?

(clue: what type of task was changing credentials, and is the same true for getting connected & online?)

Achieving a good *fit* examples:

- Automating security, for instance, using **implicit authentication** to recognise authorised users, instead of requiring them to enter passwords many times over.
- If explicit human action is necessary in a security task, we should **minimise the work-load** and the disruption to the primary task.
- Designing processes that trigger security mechanisms such as authentication **only when necessary**.
- Design systems that are **secure by default** so that they do not push the load of security configurations and management on to the users.

[note: usable security talks mainly to users, we discuss this push back to designers in error]

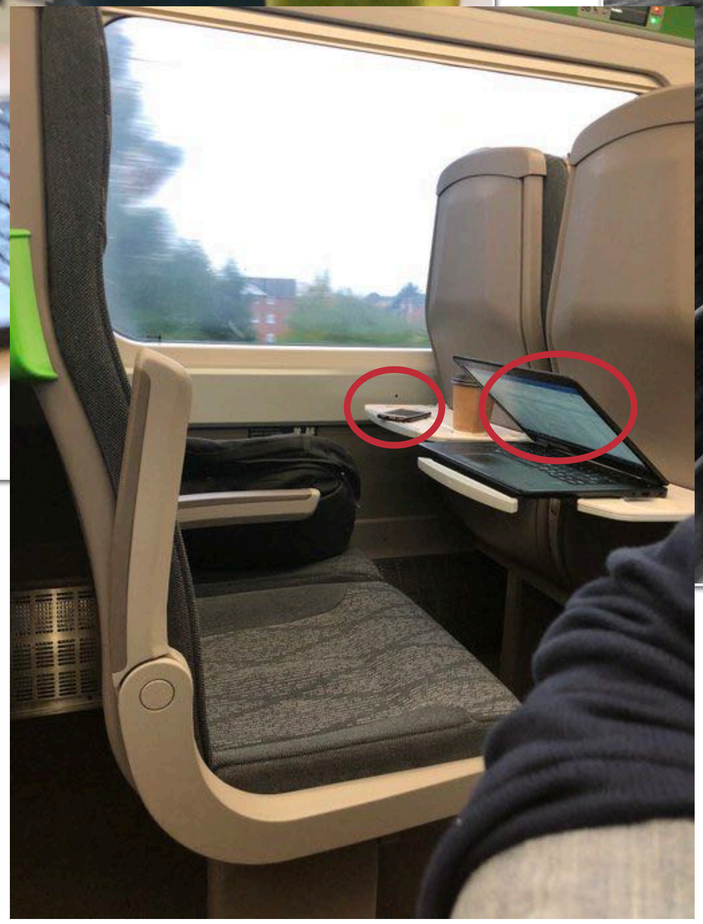
3 - The context

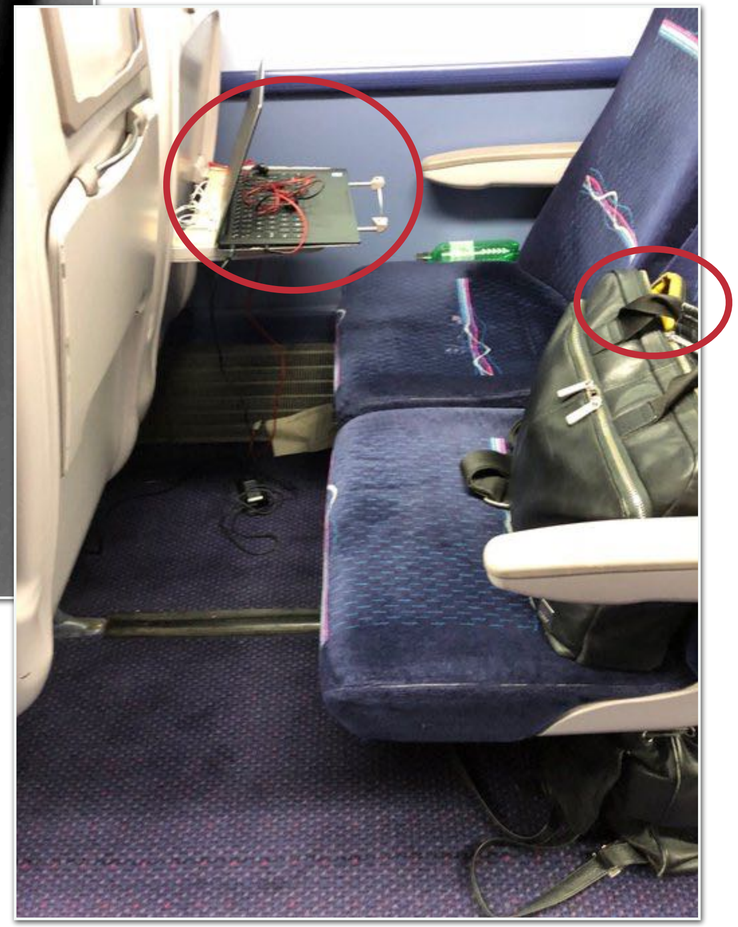
“Both the physical surroundings and the social environment in which people have to perform security tasks affect performance and security.

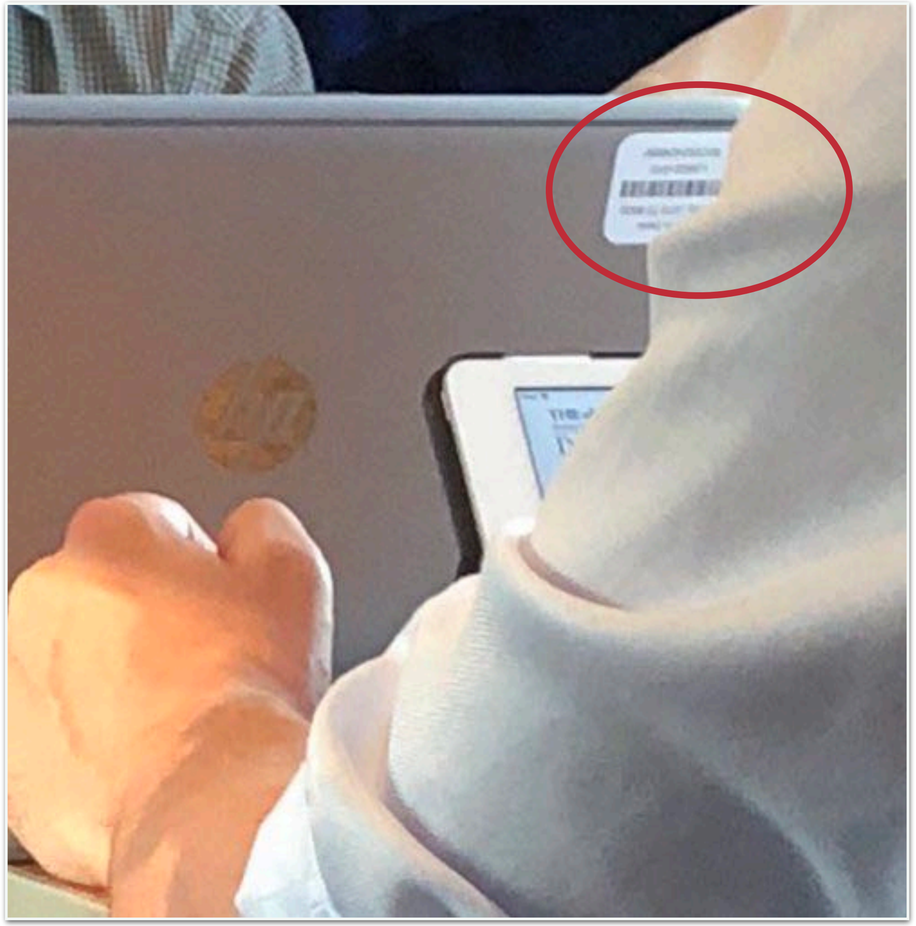
Most working age people now interact with technology on the move more frequently than at the desk traditional working environments.

This change in the context of use affects a number of security mechanisms, not least of being overheard when on the phone – the case of former CIA Director Michael Hayden being overheard giving an off-the-record interview on board a train being a particularly spectacular one.”

CyBOK








IBM Security
IBM Security Summit

Be more aware of physical context

The usability of security mechanisms can be affected by the following physical characteristics:

- Light: In bright light, displays can be hard to see, which can affect graphical authentication in particular. Biometric systems such as iris and face recognition rely on input from cameras. Bright light can lead to glare, which means the images captured are not good enough to process.

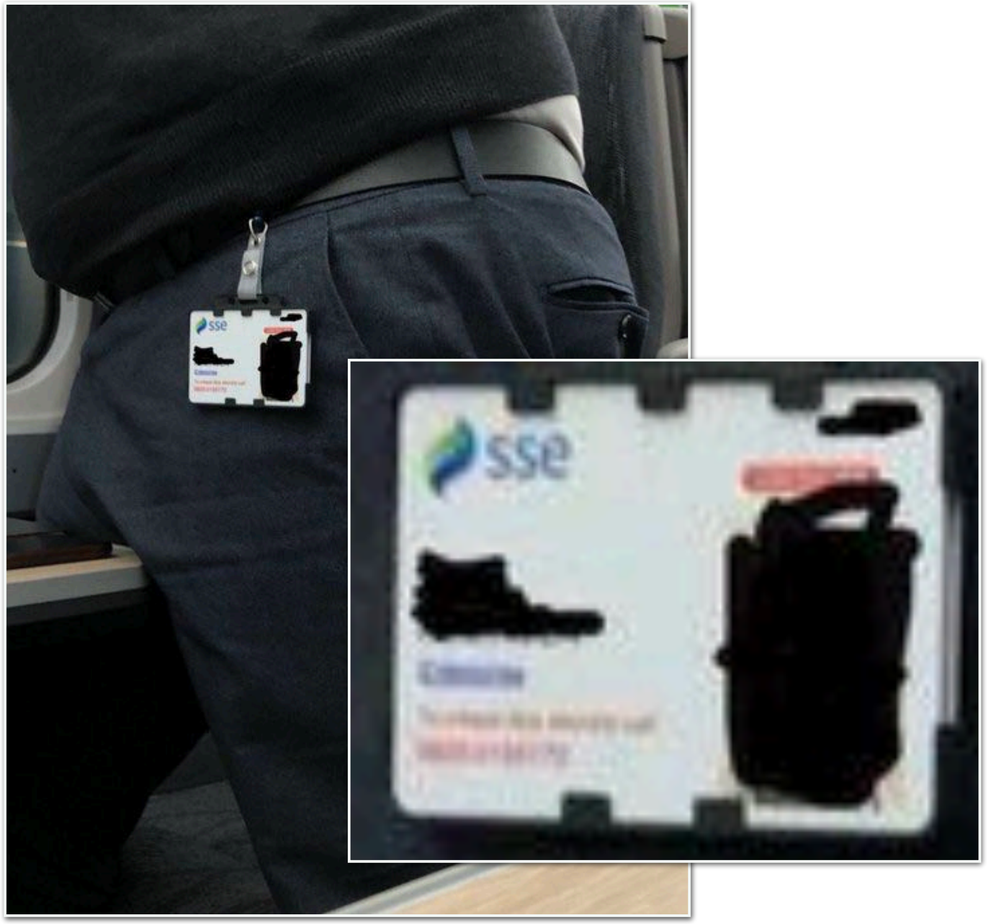
- Noise will most obviously interfere with the performance of voice recognition systems. But high levels of noise also impact human performance in general due to increased stress and, in turn, increased likelihood of error. Unexpected loud noises trigger a human startle response, which diverts attention away from the task.

- Ambient temperature can affect the performance of both technology and humans. Fingerprint sensors can stop working when it is cold, and humans are slower at pointing and selecting. They may also need to wear protective clothing such as gloves that make physical operations of touchscreens impossible or difficult. Similarly, too hot an environment can lead to discomfort and sweat can interfere with sensors.

- Pollution can impact equipment operated outdoors. This is a particularly concern for fingerprint sensors and touchscreens. The lipids left behind combine with the particles and the resulting dark grease can clog sensors or leave a clearly visible pattern on the touchscreen.

CyBOK

We need to cater for the social context



"The social context in which people find themselves **strongly influences behaviour though values**:

shared beliefs about what is **important** and **worthwhile**, and **norms**:

rules and expectations about actual behaviour.

If the expected security behaviour is in conflict with day-to-day behavioural norms, we can expect problems.

For instance, if an organisation values customer satisfaction, and employees are told to be friendly towards customers at all times, a security policy that requires staff to treat any customer enquiry as a potential attempt to extract information will not fit."

CyBOK

4 - Device Capability

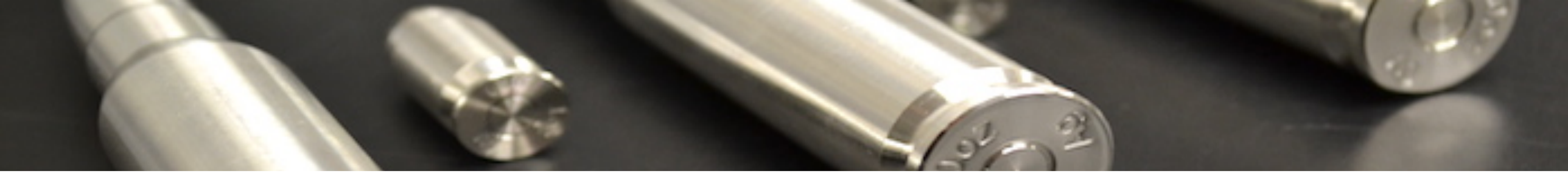
“Some characteristics of the device can result in security mechanisms becoming difficult to use in any circumstance. Entering long and complex passwords on soft keyboards on a mobile phone takes far longer and is more error-prone than on a regular keyboard”

We’ve already briefly mentioned how passwords managers can make diverse passwords more usable. Similarly we talked about the ephemeral nature of one-time authenticators & the link to STM.

Now think to the user entering a long password on an **E.161 keypad!**

Quick worked example

- 15 random char pw = rlrdF@!u06Sx!90
- replace symbols & no uppercase = rlrdf34u06sx590
- 77 5 333 3 3333 4444 88 0 6666 777 99 5555 9999 0000 **(39 characters!)**



Is Usable Security the Silver-Bullet?

In my opinion usable security **alone** isn't going to address many of the challenges in human-centred security behaviours **BUT** it plays a very significant role.

Whilst usable security is clear in it's aim to push towards security "*delivering the required levels of security and also user effectiveness, efficiency, and satisfaction*" it does clearly talk to the user's needs and how developers need to take these in to account. However, little is made of the role that developers, themselves, have in also being users of the very tools which they are using to build things.

Another critique points to the lack of user motivation and how merely being "usable" can mask security challenges for the human - remember these from HiL?

(clue: think back to Mirai again and the usable tools that masked something)

Useful Stuff

Caputo, D et al. 2016
Barriers to Usable Security? Three Organizational Case Studies
https://ieeexplore.ieee.org/abstract/document/7676139

Theofanos, M. 2020
Is Usable Security an Oxymoron?
https://csrc.nist.gov/CSRC/media/Projects/usable-cybersecurity/images-media/Is%20Usable%20Security%20an%20Oxymoron.pdf

Complimentary “…by Design” frameworks

Many of the critiques of Usable Security are based around it being treated as in some way standalone, or an unbending doctrine.

However, the reality is Usable Security can work well especially when combined with one or more of the ‘be Design’ frameworks which look more broadly and holistically.

Privacy by Design
Guidelines developed in the 1990s by the then privacy commissioner of Ontario, Ann Cavoukian. The movement seeks to embed privacy "into the design specifications of technologies, business practices, and physical infrastructures".

Security by Design
Guidelines to implement security from the ground up resulting in software has been both designed and built to minimise flaws that could compromise security.

Security Ergonomics by Design
Guidelines that empower software engineers to pragmatically take into account how users (including themselves) make informed security choices about their data and information when building safe and secure cyber physical systems.

Useful Stuff

Cavoukian, A. 2009
Privacy by Design: The 7 foundational principles
http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf

NCSC
Secure Design Principles
https://www.ncsc.gov.uk/collection/cyber-security-design-principles

Craggs, B & Rashid, A. 2017
Beyond Usable Security to Security Ergonomics by Design.
https://ieeexplore.ieee.org/iel7/7965809/7967966/07968021.pdf

A Task

Pick **ANY** security tool (other than a password manager!) and, based on your **own** experience, see if you can answer the three usability measures for it:

- **Effectiveness** "Can users achieve their goals?”
- **Efficiency** "What resources are expended to do so?”
- **Satisfaction** "What is the user level of comfort and acceptability?"

next time…
Inclusive Security