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

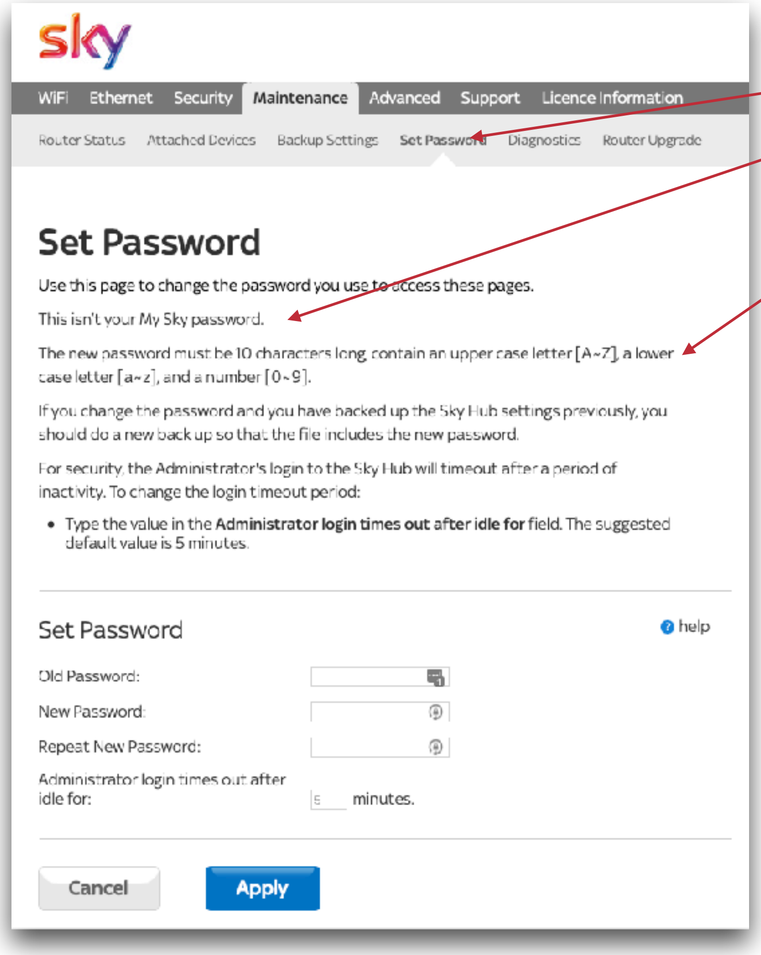
110 Expert authors, reviewers and advisors
828 Pages long
1,839 Authoritative sources

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outdated structure guidance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

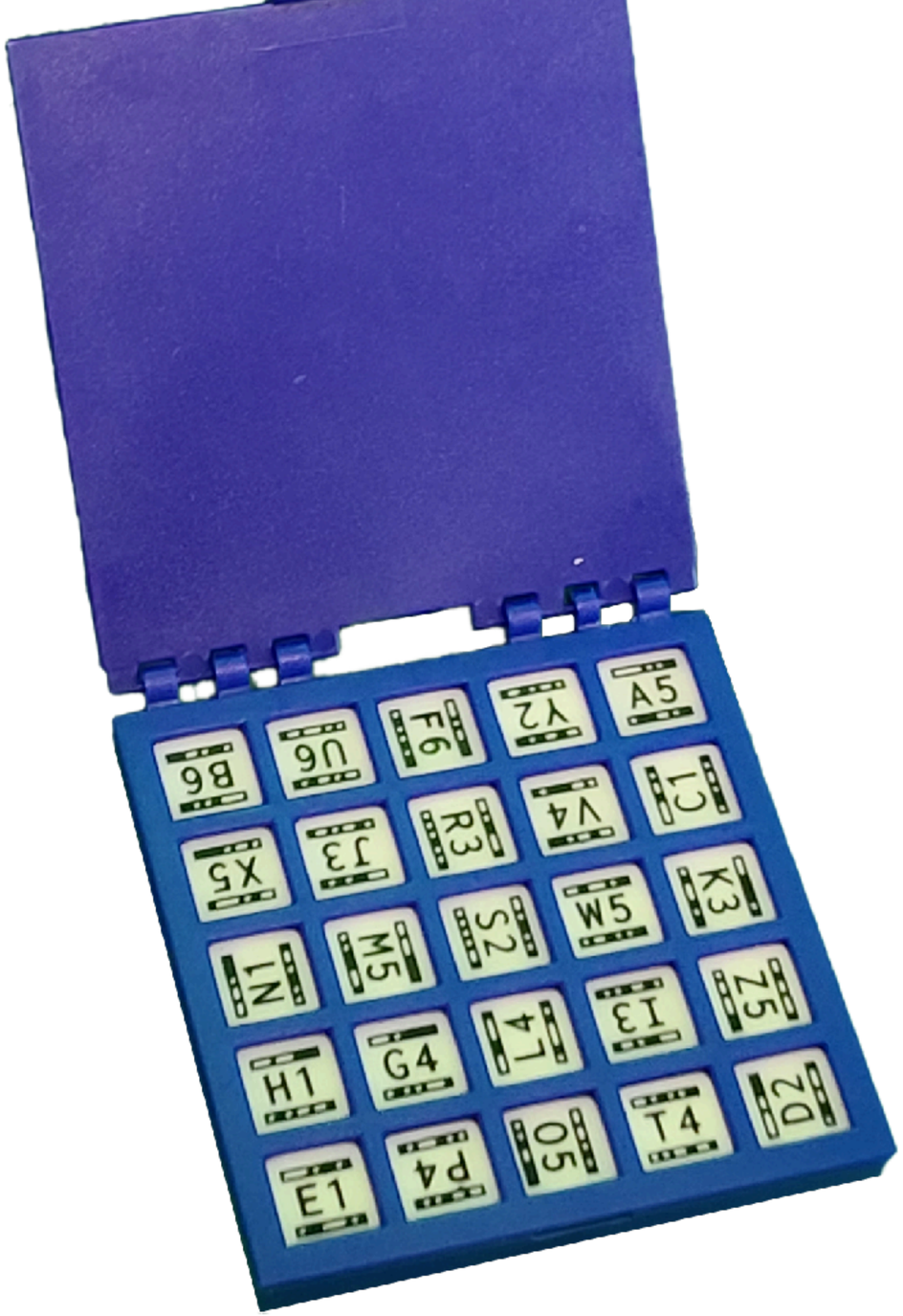
Can you remember 15 random characters for every site? We're back to human capacity issues and their workarounds.

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)
Next…