Cyber Security Body of Knowledge: Human Factors

Awais Rashid
Bristol Cyber Security Group
University of Bristol, UK

bristol.ac.uk
The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.
Less that 0.1% of email is end-to-end encrypted!

Users are not the Enemy!

Fit the human to the task
Fit the human to the task

Fit the task to the human

bristol.ac.uk
Security has to be usable

*Effectiveness*: Can users achieve their goals?

*Efficiency*: What resources are expended to do so?

*Satisfaction*: What is the level of comfort and acceptability for users?
This knowledge area introduces a broader organisational perspective on security that has emerged over the past decade: the importance of trust and collaboration for effective cyber security, which can only be achieved by engaging stakeholders and negotiating security solutions that meet their needs. This requires a set of skills that have traditionally not been part of the training provided for security experts and practitioners. This knowledge area aims to capture the knowledge to change that.

This is organised in a way starting on the inside, working outwards: starting with the individual and internal factors that drive human behaviour (capabilities and limitations, mental models), moving onto aspects of the broader context in which interaction with security takes place. We will then consider the other immediate factors that have an impact: the behaviour of others around us, and especially how they handle security risks, users' emotional states towards the organisation and how security behaviour can be successfully managed through design and a range of group and organisational factors.

Note that human actors and usability in a security context can be distinguished from other contexts by the presence of adversaries or risk. As shown in Figure 1, the adversary may actively work to alter users' perceptions of the system's capabilities and boundaries as well as exploiting the specifics of social and organisational contexts (e.g., security policies, 4).
Human Capabilities and Limitations

- Alarm Fatigue
- STM vs. LTM
- Strength Meters
- CAPTCHA

bristol.ac.uk
Compliance Fatigue
Latent Design Conditions

bristol.ac.uk
“Never give an order that can’t be obeyed”

General MacArthur

Never issue a security policy that cannot be followed
Awareness and education

- Safe behaviour
- Acceptance
- Implementation (skills / abilities)
- Conviction (positive perception / attitude)
- Understanding/Knowledge
- Sensitising
- Information

Covered by extra commitment of the company

Covered by ISO 27001: A.7.2.2 Information security awareness, education and training

bristol.ac.uk
Mental models of cyber security and risks
What about developers?
What Usability Issues Do Developers Face?

- Should I use this?
- How should I use this?
- Build Issue
- Performance
- Passing the buck
- Lack of Knowledge
- Unsupported Feature
- Borrowed Mental Models
- Usage Issues
- System Issues
- Not knowing what to do
- Not knowing if it can do
- Missing Documentation
- Looking for Example Code
- Clarity of Documentation
- Abstraction Issue
- What’s gone wrong here?
- API Misuse
- Compatibility Issue
- Deprecated Feature
- Missing Information
- Programming is hard
- Issues across time and space

Developers are Not the Enemy! 
The Need for Usable Security APIs

Matthew Green and Matthew Smith

bristol.ac.uk
Principles for Usability of Crypto APIs

Abstract: Integrate cryptographic functionality into standard APIs so regular developers do not have to interact with cryptographic APIs in the first place.

Powerful: Sufficiently powerful to satisfy both security and non-security requirements.

Comprehensible: Easy to learn, even without cryptographic expertise.

Ergonomic: Don’t break the developer’s paradigm.

Intuitive: Easy to use, even without documentation.
Principles for Usability of Crypto APIs

Failing: Hard to misuse. Incorrect use should lead to visible errors.

Safe: Defaults should be safe and never ambiguous.

Testable: Testing mode. If developers need to run tests they can reduce the security for convenience.

Readable: Easy to read and maintain code that uses it/Updatability.

Explained: Assist with/handle end-user interaction, and provide error messages where possible.

bristol.ac.uk
Usability Smells: An Analysis of Developers' Struggle With Crypto Libraries

Nikhil Patnaik, Joseph Hallett and Awais Rashid
Fowler’s Shotgun Surgery

“You whiff this when every time you make a kind of change, you have to make a lot of little changes to a lot of different classes. When the changes are all over the place, they are hard to find, and it’s easy to miss an important change” – Definition of Shotgun Surgery
1 **Need a super-sleuth**

You whiff this when documentation is missing, unclear or there is a lack of example code pertaining to how to use the library.

3 **Needs a post-mortem**

The developer has used the library but something has gone wrong. Either they have used the library incorrectly or they are struggling to work out if it is an issue with the library itself.

2 **Confusion Reigns**

You can catch a whiff of this when developers are designing and prototyping their programs—they are trying to decide whether this is the right library to use and how to start using it.

4 **Doesn’t Play Well With Others**

This smell occurs when the library won’t build, won’t integrate with other libraries and build systems, and is a resource hog without providing a clear explanation why.
and acceptable to a range of human actors, for instance, end-users, administrators and developers. This knowledge area also introduces a broader organisational and societal perspective on security that has emerged over the past decade: the importance of trust and collaboration for effective cyber security, which can only be achieved by engaging stakeholders and negotiating security solutions that meet their needs.

This requires a set of skills that have traditionally not been part of the training provided for security experts and practitioners. This knowledge area aims to capture the knowledge to change that.
Fit the human to the task

Fit the task to the human