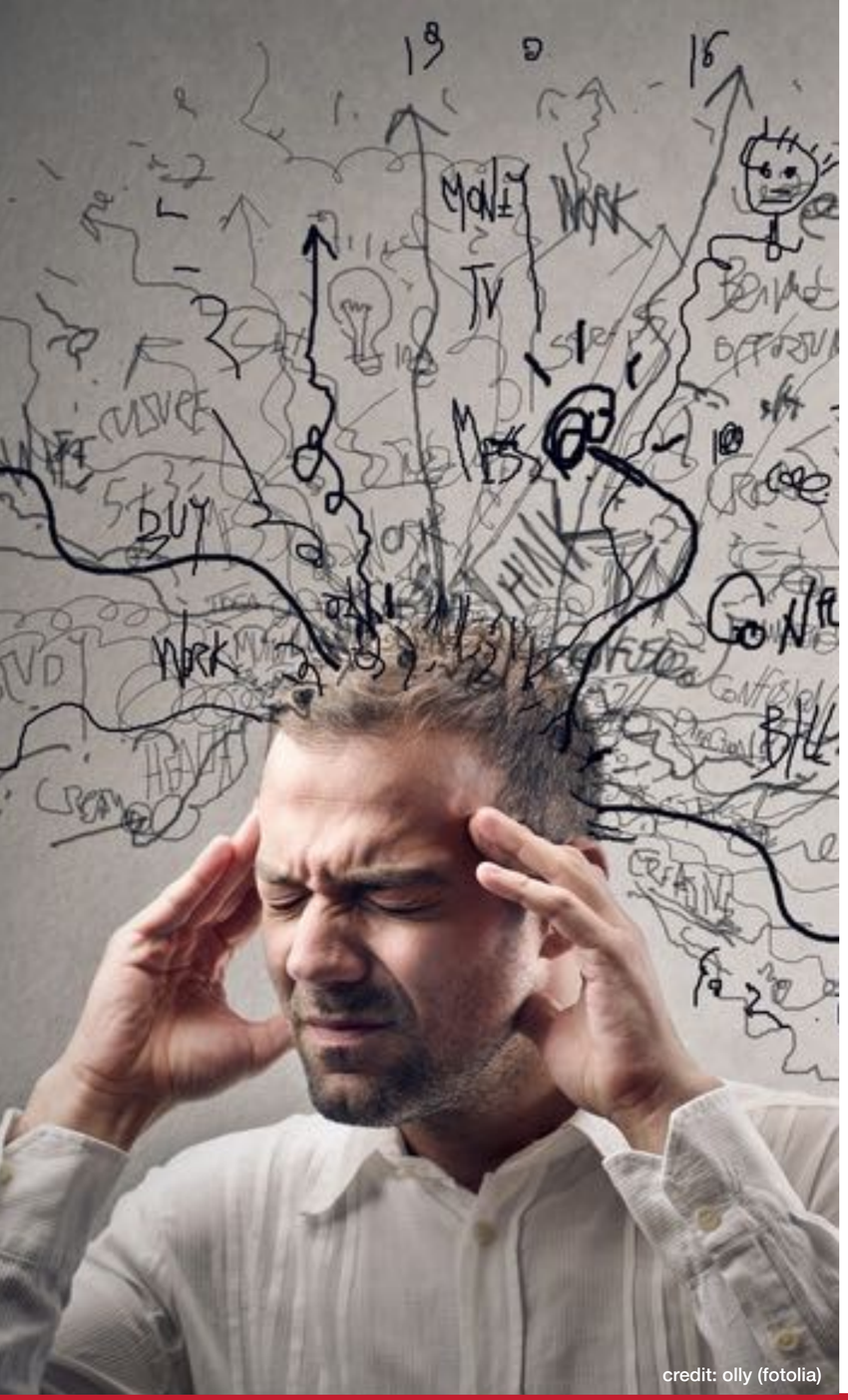
Security Behaviours

COMS30038 Lecture 7 - Inclusive Security

Dr Ramokapane

University of BRISTOL

Bristol Cyber Security Group



Quick Usable Security Recap

Usability is "**the effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments.**" ISO 9241-11:2018

We assess usability by -

- **effectiveness**: the accuracy and completeness with which specified users can achieve specified goals in particular environments
- **efficiency**: the resources expended in relation to the accuracy and completeness of the goals achieved;
- **satisfaction**: the comfort and acceptability of the work system to its users and other people affected by its use.

Making security tasks fit the human means accounting for -

1. the **capabilities** and **limitations** of the target users;
2. the **goals** those users have, and the **tasks** they carry out to achieve them;
3. the **physical** and **social context** of use; and
4. the **capabilities** and **limitations** of the **device** on which the security mechanism is used

Inclusive security (Part A…)

Usability is necessary — inclusion makes it complete.

! Reading !

From usability to inclusivity…

This visionary paper calls for a *third wave* of security and privacy research, one that is centered on **inclusion**. Building on decades of work in technical security (the first wave) and usable security (the second wave), Yang Wang introduces *inclusive security and privacy* as a new paradigm that treats human diversity of ability, identity, culture, and values as first-class design requirements.

Wang argues that security and privacy mechanisms must serve everyone, not just the average user, and presents a research framework grounded in **universal design**, **accessibility**, and **value-sensitive design**.

Useful Stuff

Wang, Yang. "The third wave? Inclusive privacy and security." *Proceedings of the 2017 new security paradigms workshop*. 2017.

Renaud, Karen, and Lizzie Coles-Kemp. "Accessible and inclusive cyber security: a nuanced and complex challenge." *SN Computer Science* 3.5 (2022): 346.

Sannon, Shruti, and Andrea Forte. "Privacy research with marginalized groups: what we know, what's needed, and what's next." *Proceedings of the ACM on Human-Computer Interaction* 6.CSCW2 (2022): 1-33.

Das Chowdhury, Partha, et al. "From utility to capability: A new paradigm to conceptualize and develop inclusive pets." *Proceedings of the 2022 New Security Paradigms Workshop*. 2022.

From Usability to inclusivity

Usable Security: fit tasks to the human.

But — which human?

Many “usable” systems are usable only for *some* people.

Inclusive security broadens usability to *equity of access* and *fairness of protection*.

From Usability to inclusivity

Concept	Core Question	Focus	Goal
Usability	*Can the user complete the task effectively, efficiently, and satisfactorily?*	Interaction quality and human performance	Reduce friction and cognitive load for the **intended user**
Accessibility	*Can people with diverse physical, sensory, or cognitive abilities access and use it?*	Equitable access; technical and physical enablement	Remove barriers so **people with disabilities** can participate equally
Inclusivity	*Does the system work fairly and safely for **all users**, across abilities, cultures, genders, languages, and contexts?*	Diversity, context, and equity of protection	Ensure **no one is excluded** or placed at greater risk by design assumptions

Usability focuses on *ease* — fitting the task to the human.

Accessibility ensures *ability* — enabling interaction for everyone.

Inclusivity ensures *equity* — designing systems that protect and empower all users fairly.

What is inclusive security?

Useful Stuff

Designing systems that are accessible, fair, and usable for *all* users.

Moves beyond compliance toward empathy & participation.

Inclusivity is not just about accessibility: inclusion means designing for diversity of ability, culture, and context.

Goal: *Equal security outcomes for unequal contexts.*

Why Inclusion Matters for security?

Useful Stuff

Exclusion leads to **unsafe workarounds** (e.g. shared passwords).

Security that only fits privileged contexts creates vulnerabilities.

Insecurity spreads — weakest links matter.

Inclusion = resilience.

Usability ≠ Neutral?

“Usable” for whom?

Default assumptions: sighted, literate, able-bodied, English-speaking, digitally connected.

Ignoring diversity = latent failure baked into design.

Useful Stuff

Exclusion as Latent Failure

Latent failure refers to ***dormant weaknesses in a system, such as poor design, inadequate training, or flawed procedures, that lie hidden until they contribute to an "active failure" or human error, leading to an accident.***

- Connect to Reason's model: active vs. latent failure.
- Exclusion is **a system-level latent flaw** that manifests when real humans interact.
- When usability assumes sameness, error is inevitable.

CAPTCHA that relies only on vision

→ excludes blind users

→ they delegate security.

Useful Stuff

Who Gets Left Out

Dimension Example

Physical - Fingerprint sensors fail with prosthetics or gloves

Cognitive - MFA timeouts too fast for neurodiverse users

Cultural/Linguistic - English-only warnings misread in localisation

Socio-economic - Security apps assume constant connectivity

Gender and Identity - Threat models ignore coercive control scenarios

Age - Motor skills, memory, device familiarity differ

Useful Stuff

Renaud, Karen, and Lizzie Coles-Kemp. "Accessible and inclusive cyber security: a nuanced and complex challenge." *SN Computer Science* 3.5 (2022): 346.

Real-World Failures

System/Example	Who Was Excluded	Security Consequences
Multi-Factor Authentication apps (Google Authenticator, banking apps)	Users without smartphones or with motor impairments	Forces users to rely on SMS or single-factor logins which may weaken the overall security posture.
Facial recognition	Darker-skinned and female faces	Leads to higher false rejections / approvals which leads to unfair denial of access. There is also potential for profiling.
Voice biometrics	Women and older users – trained mostly on male voices	Authentication errors and lockouts forcing users revert to weaker password recovery methods.
“Safe” browsing features in shared-device contexts (domestic abuse cases)	Survivors/Victims of coercive control or surveillance	“Incognito” mode or auto-logins can expose private activity. They can pose risk despite being “secure.”
Audio & visual CAPTCHAs	Users with hearing or visual disabilities	Unable to complete verification. Users may resort to unsafe delegation (e.g. sharing passwords).

Exclusion becomes insecurity. It is not just unfair, but creates new attack surfaces.