# Inclusive security (Part B...)

You build what you believe...

# Encoding Bias in Security Systems

“Bias isn’t only in data — it’s in every decision about who the system is built for.”

**Human → Assumption → Design → Outcome.**

- Every system reflects the assumptions of its **designers** and **context**. Designers’ biases often leads to system biases.
- Decisions about what is “normal,” “secure,” or “user-friendly” are **value choices**.
- When those choices ignore diversity, they **bake in bias** even unintentionally.
- Inclusive design = anticipatory bias mitigation. Inclusive design means **questioning assumptions early**, not just fixing problems later.

| Design Decision | Assumption Made | Impact / Risk |
|---|---|---|
| *Login requires mobile number* | *Everyone owns and carries a personal phone* | *Excludes low-income or shared-device users* |
| *Fingerprint scanner* | *Everyone has readable fingerprints* | *Fails for manual laborers, elderly, or prosthetic users* |

# Different Threat Models, Different Realities

Security threats are not universal, they differ by user identity. Context matters and inclusion recognises these differences. Security is not a one-size-fits-all, it must adapt to human diversity.

Inclusive security is not only about accessibility. It is about *situated safety*. It’s designing mechanisms that **flex with context** instead of enforcing a rigid idea of how everyone should behave.

“The ‘average user’ does not exist.”

Inclusive systems empower users to manage their own risk, instead of assuming a single definition of safety.

Inclusive systems adapt, not dictate. A design that feels secure in one context can be dangerous in another.

# Different Threat Models, Different Realities

| User Context | Primary Risks/Threat Model | Design Implications |
|---|---|---|
| Software Engineer (office environment) | Credential theft, phishing, corporate espionage | Strong MFA, phishing-resistant flows, minimal disruption to productivity |
| Human Rights Activist (under surveillance) | State monitoring, device seizure, metadata tracking | Stealth/duress modes, local encryption, minimal cloud sync, anonymous comms |
| Teenager (social media ecosystem) | Oversharing, coercion, peer pressure, exploitation | Privacy defaults “on”, safety prompts, consent education |
| Older Adult (home or caregiving context) | Fraud, impersonation scams, cognitive overload | Simplified UI, clear warnings, trusted contact recovery, large-print accessibility |

# Inclusion Strengthens Resilience

**Inclusive systems are more resilient systems.**
*When security design accounts for diversity of people, contexts, devices, and abilities. It becomes harder for failures, exploits, or exclusions to cascade.*

## Diverse design = fewer blind spots.

- Homogeneity breeds fragility. When design teams share similar backgrounds, they often miss entire categories of user behaviour or threat models.
- **Diversity functions like redundancy in engineering.** Each perspective catches different potential points of failure.

## Accessibility improves everyone’s usability.

- Accessibility features **rarely help *only* those with disabilities,** they improve general UX.
- Accessibility = **universal usability under stress**, which directly supports operational security.

“The better you design for edge cases, the stronger your baseline usability becomes.”

## Inclusion supports trust, compliance, and adoption.

- People adopt what they trust and they trust **what reflects *them***. If users feel a system excludes or misunderstands them, they would not comply with its rules. *Example*: Users locked out by face recognition bias lose trust and may turn off or bypass the system.
- Inclusion thus supports the **social contract** between users and security: “I follow your guidance because it’s clearly for people like me.”

## Diversity is a security control.

- **Traditional controls**: authentication, encryption, audit logs.
- **Human-centred controls**: diversity, participation, and fairness. They make systems more robust to social engineering, insider misuse, and design bias.
- Diverse perspectives in **threat modelling** reveal different risks. Each insight closes a gap an attacker might exploit.

# Principles of Inclusive Security by Design

### Equitable Access

no unnecessary barriers to protection.

### Flexibility

multiple secure pathways (e.g. recovery options).

### Transparency

communicate clearly, across languages & literacy levels.

### Participation

co-design with diverse stakeholders.

### Context Sensitivity

adapt to environments and users' lived realities.

# Inclusive Interventions

- Plain-language communication.
- Accessibility audits beyond compliance.
- Culturally localised UX cues.
- Alternative authentication paths (hardware keys, codes, passphrases).
- Community consultation in threat modelling.

# Reflection

Who is your “default” user?

Who is invisible in your design?

Who bears the cost of your security decisions?

# Takeaways

**Usability ≠ Universality**
Security that works for some users may fail or endanger others.

**Exclusion is a Latent Failure**
Designs that ignore diversity create hidden vulnerabilities.

**Accessibility Enables, Inclusivity Empowers**
Accessible systems remove barriers; inclusive systems build equity and trust.

**Diversity is a Security Control**
Different perspectives reveal different risks inclusion strengthens resilience.

**Inclusive Design = Secure Design**
Systems that adapt to human difference are more trusted, adoptable, and resilient.

# A Task

Pick a common security mechanism (password reset, CAPTCHA, login, cookie consent).

- Who might be excluded?
- What small redesign could make it inclusive?

next time...

error in practice