2025 MIT STAMP Workshop

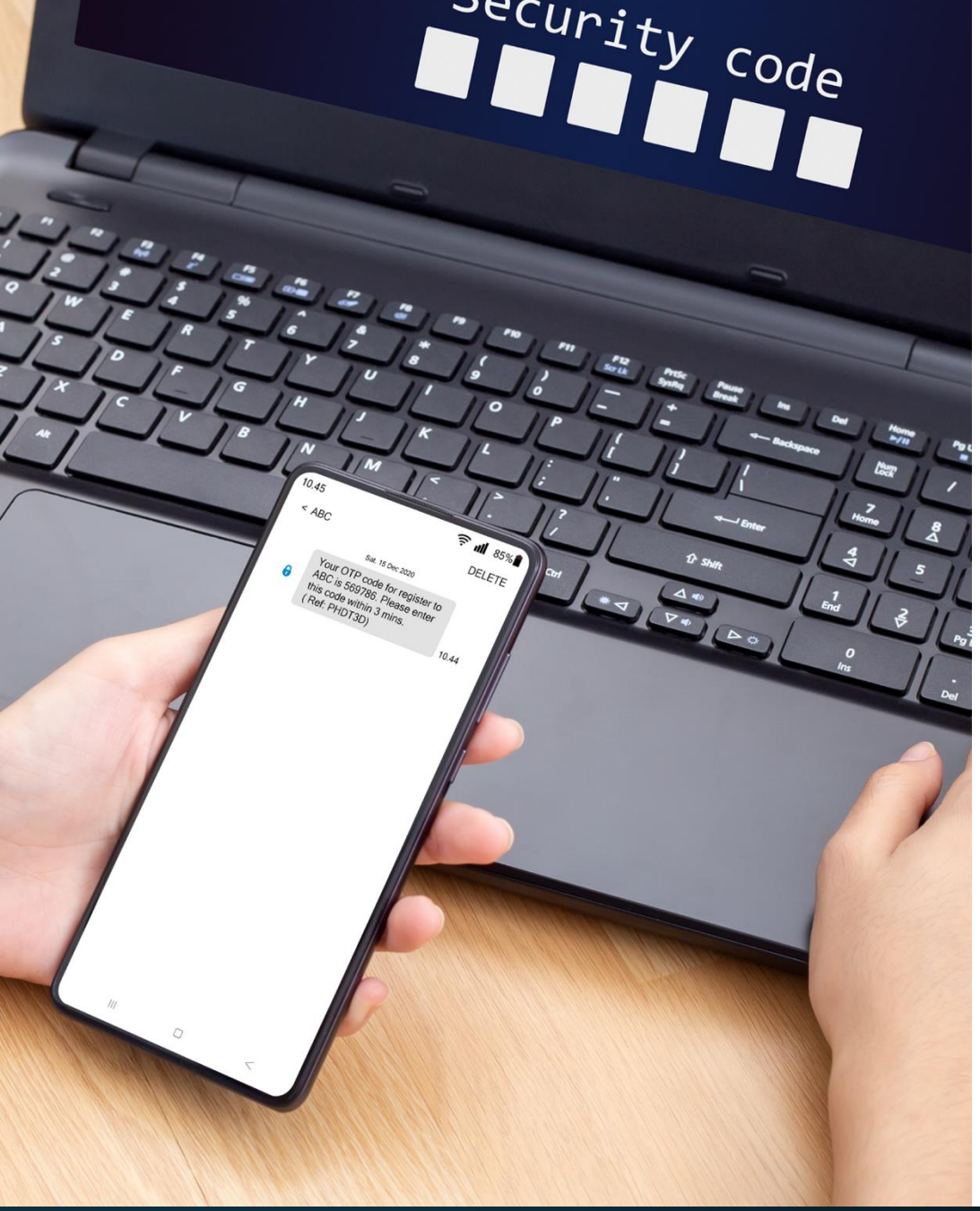
STPA of User-System Interaction in SMS-Based MFA: Differentiating Legitimate Errors from Security Threats

Presenter: Jeni Rahman
Supervisor: Ashley Brooks

MSc Security and Resilience: Science and Technology
Imperial College London

IMPERIAL

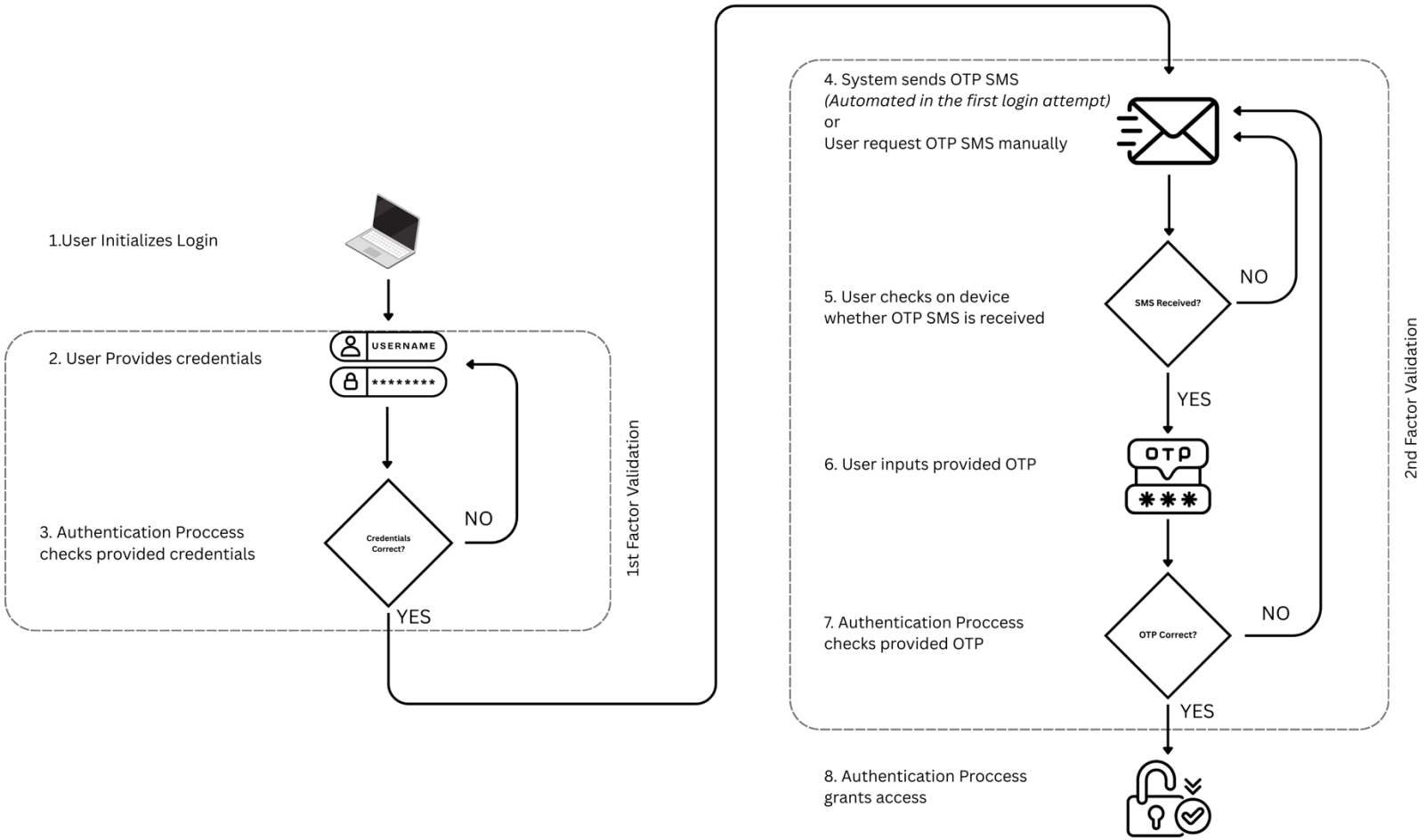
IS THAT YOU ?



Why still use SMS-Based MFA?

- Built-in on every phone
- Ready to use
- User familiarity
- No internet required
- Easy & quick to deploy

LIMITATIONS AND VULNERABILITIES



- Device dependency (active number)
- Delivery delays (network connection, involving other entities: Mobile Network Operator & SMS Gateway)
- User input errors (user-system interaction)
- Vulnerable to SIM swap attacks interception risks

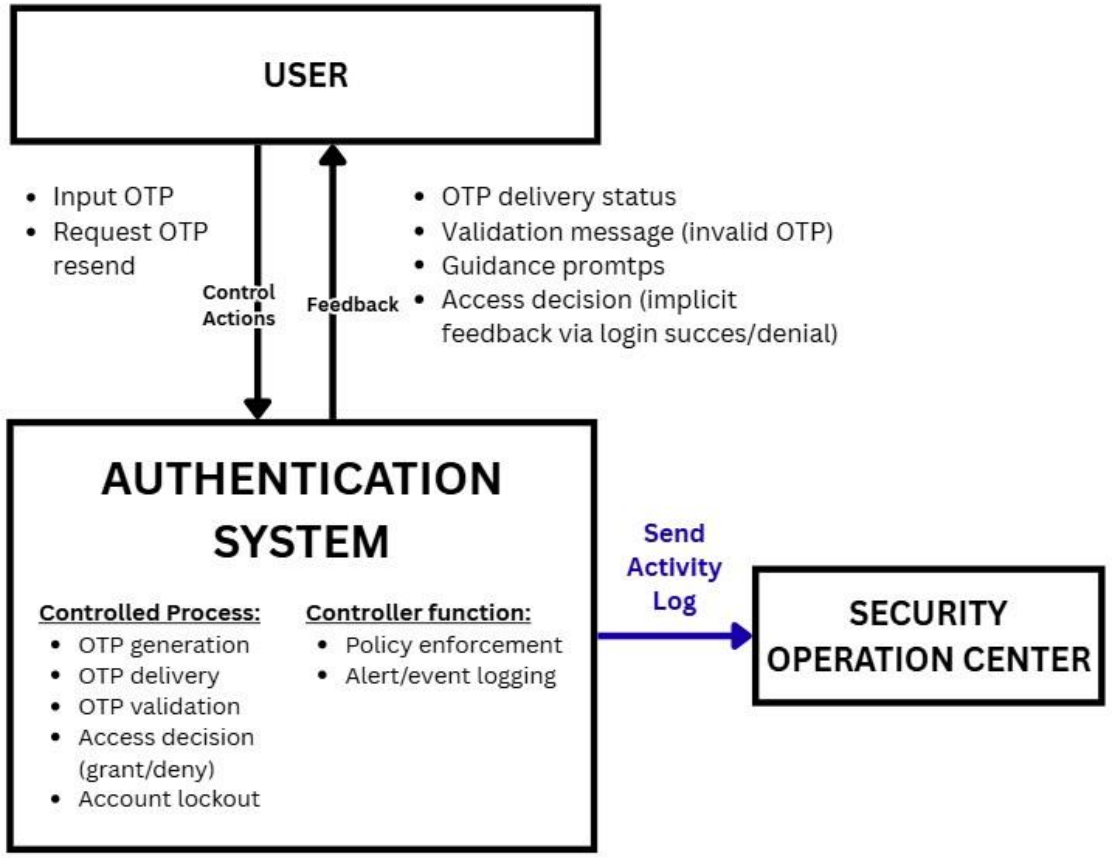
STPA Application

Focus on User-System Interaction



- Examines how common user's unsafe control action can create hazards such as ***account lockout***
- **Account lockout** is a common security policy to prevent brute-force attacks.
- Outcome: provide insights for policy configuration and alert enhancement to reduce false positives and improve resilience
- Thresholds are typically set on failed OTP attempts (3-5 tries as recommended by OWASP).
- Account lockout, when it is actually done by legitimate user's error, can leads to many losses:
  - Productivity loss (L1)
  - Financial loss (L2)
  - Reputational loss (L3)
  - Security Operation Center inefficiency from false positive alert (L4)
- **However, not all failed OTP inputs indicate a threat.**
- Sometimes it is a result from **normal user errors.**

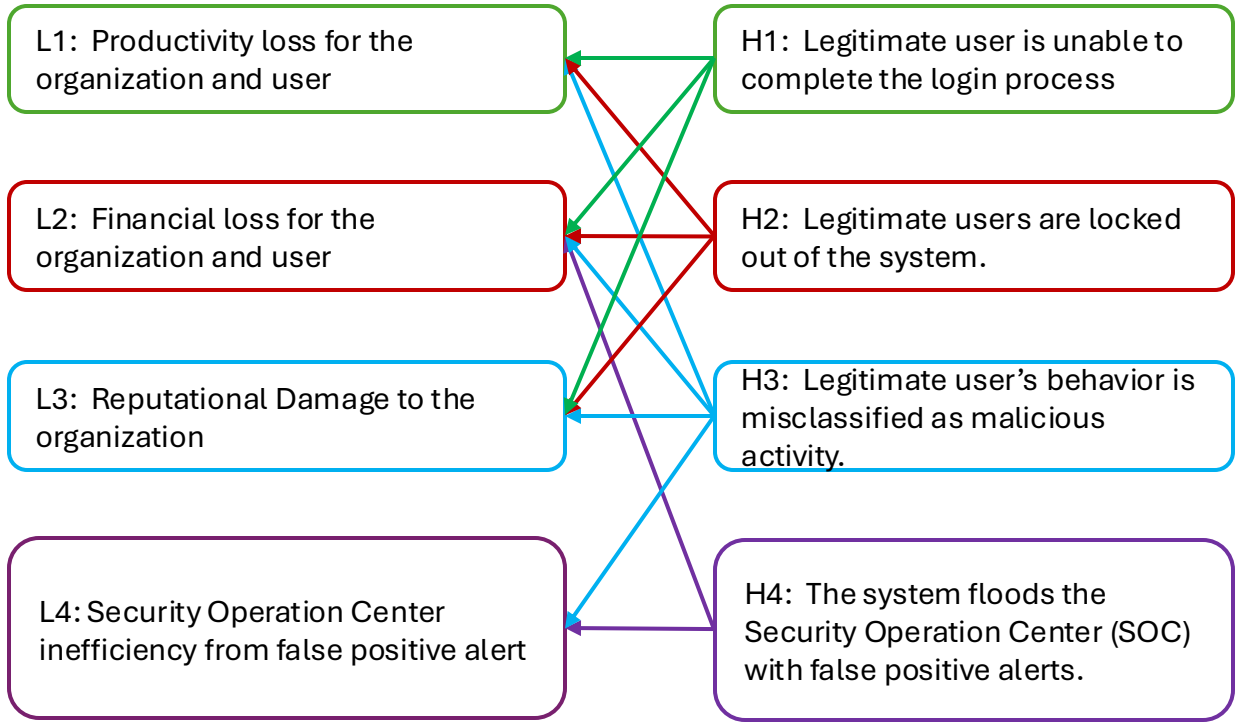
Hazard Focus: ***ACCOUNT LOCKOUT***



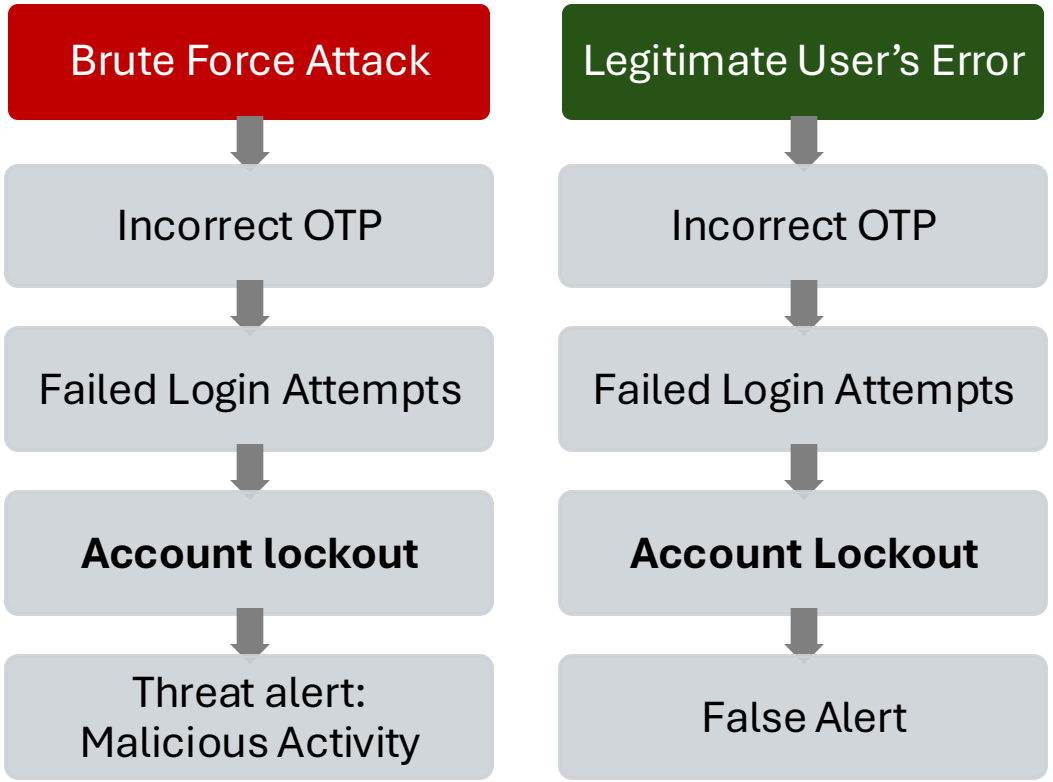
Control structure.

Losses:
Something of value to stakeholders that if unacceptable if lost.

Hazards:
System condition that can cause a loss under worst-case environment.



FINDINGS



Common user errors in OTP input:

1. Not providing OTP
2. Typo
3. Expired OTPs
4. Old OTP
5. Repeated OTP resend request

Comparison & Tolerances Configuration:

1. OTP Delivery vs. Resend Request
2. One-digit Tolerance
3. Expired vs. Delayed OTP
4. Old vs. New OTP (Previous vs. Current)
5. Resend is Not Automatically Flooding

*STPA has helped identify the causal scenario of **account** lockout, which would have been difficult otherwise and treated just generally as failed login attempts.*

IMPLICATIONS TO SOC





FAILED LOGIN ATTEMPT

Failed Login Attempt: Expired OTP

Failed Login Attempt: Input previous OTP

Failed Login Attempt: One-digit incorrect

STPA helped to identify the causal scenarios and enrich the SOC with detailed information on each failed login attempts.

VALUE & TAKEAWAY

- SMS-Based MFA has **many limitations**, including to the user's experience itself.
- Most security policy may lead to hazards and losses if **it's not configured well**.
- Despite the limitation, we **can control the system** to differentiate the legitimate user's error and the potential threat (e.g. brute force attack)
- STPA helps to create detailed policy configuration and alert system.

- **Opportunity:**
  More detailed focus on an MFA system can discover more UCAs which would identify the more system constraints to design a better systems, especially in understanding the user's behavior.
- The STPA analysis can help to enrich the automation in user and entity behavior analytics (UEBA)

IMPERIAL

Thank you!

Please get in touch!

Jeni.rahman24@imperial.ac.uk
a.brooks15@imperial.ac.uk