DESKTOP AUTHENTICATION HASN’T CHANGED MUCH
MORE THAN ONE WAY TO LOCK A PHONE

- **iOS**
  - Passcode (PIN, password)
  - Touch ID (fingerprint)

- **Android**
  - PIN/password
  - Pattern Unlock
  - Smart Locks
    - Trusted devices, face, place
    - On-body detection
Mobile devices have

- distinct use patterns
- distinct threat models
- market pressures
- vertical integration
A MODEL OF MOBILE AUTHENTICATION

Unlocked \quad \text{Authentication success} \quad \text{Locked}

Log out
A MODEL OF MOBILE AUTHENTICATION

- Unlocked
  - Authentication success
  - Short timeout
  - Button lock
  - Device rebooted

- Partly Locked
  - Authentication success
  - Long timeout
  - Remote lock enabled
  - Too many failed logins
  - Device rebooted

- Fully Locked
DOMINANT VS. SECONDARY AUTHENTICATION

- Dominant authentication always unlocks the device
- Secondary authentication sometimes unlocks the device
LAYERED SECURITY MECHANISMS

• Is having more authentication methods better for security?
  • Authentication methods are keys more than doors

• How to calibrate the security differences between dominant and secondary authentication?
  • Lockout policies are the usual approach
  • Many aspects of lockout policies are user-configured
A CHOICE OF AUTHENTICATION SCHEMES

• New models leave the choice of authentication mechanisms in the hands of the user
• Do people know how to choose and configure the right security for them?
FUTURE AUTHENTICATION STRATEGIES

- How will this model develop?
- Continuous authentication?
- What design opportunities are facilitated by this authentication model?
- Partial authentication?
- Per-app authentication?
OPEN QUESTIONS

• What are the security implications of layering multiple authentication mechanisms?
• How will giving users a variety of choice in how they secure their devices play out?
• Will this model persist? How will it develop in future?

• Thank you!
• elizabeth.stobert@inf.ethz.ch