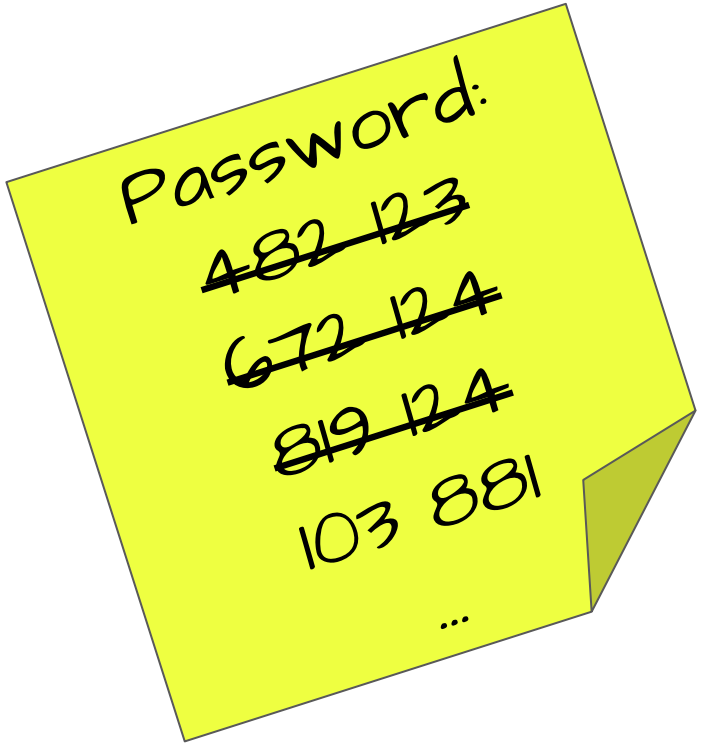
Time-Based One-Time Password Algorithm

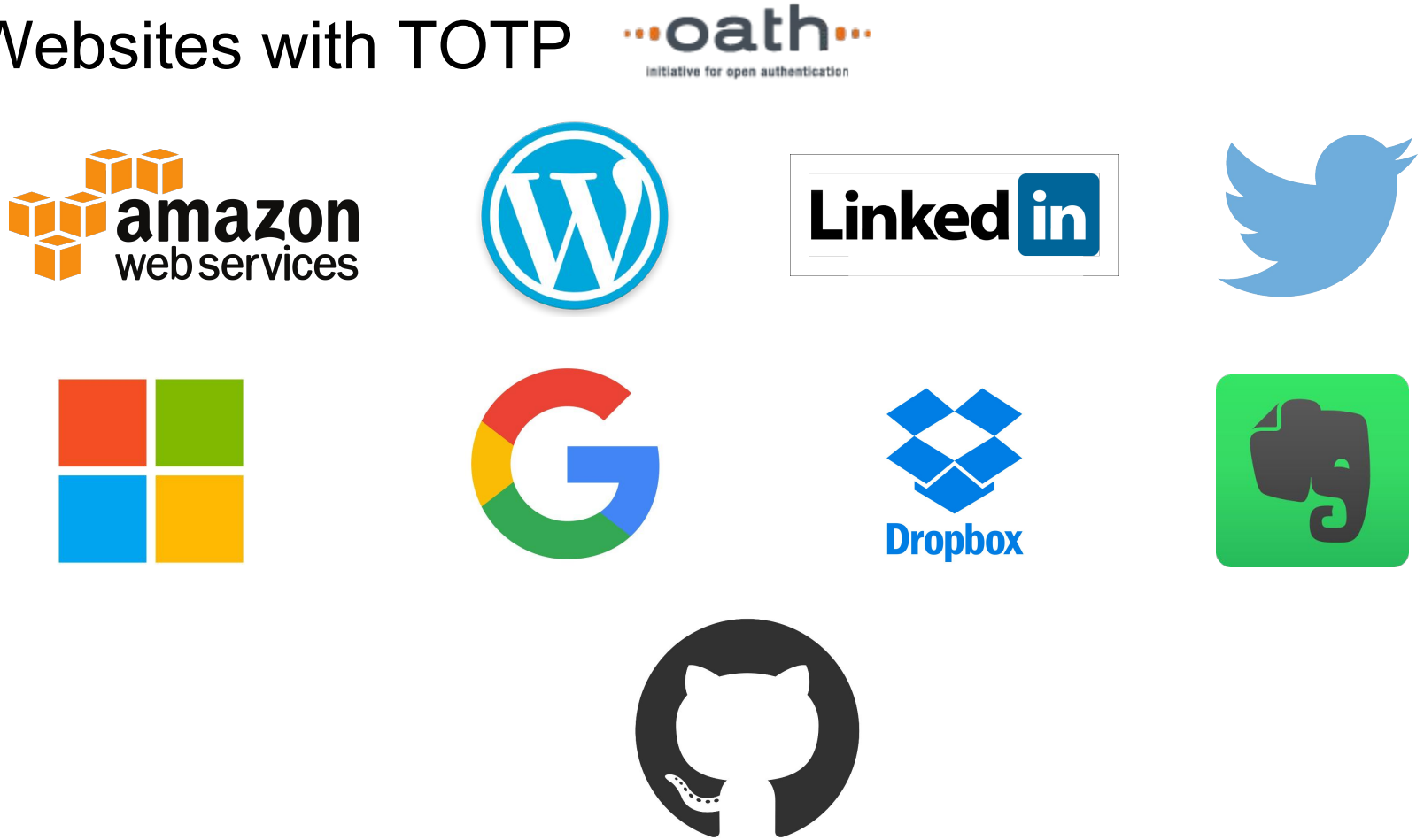
Matthew Cole, Anh Quach, Daniel Townley

Introducing TOTP

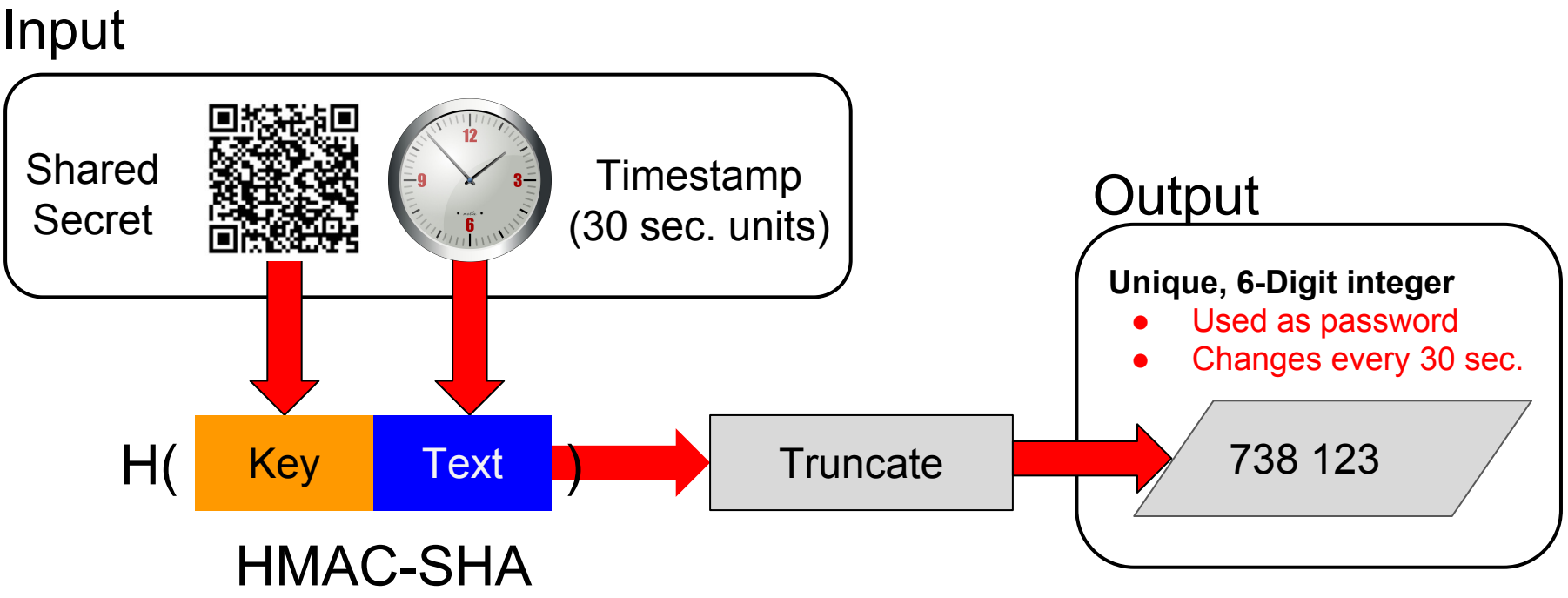
- Problem: password-based authentication invites replay attacks
- Defense: change password regularly
  - Sans Institute recommends every 3 months
  - Encourages weak passwords
  - Still enough time for replay attacks
- Can we change the password *every 30 seconds?*
  - Not as crazy as it sounds...



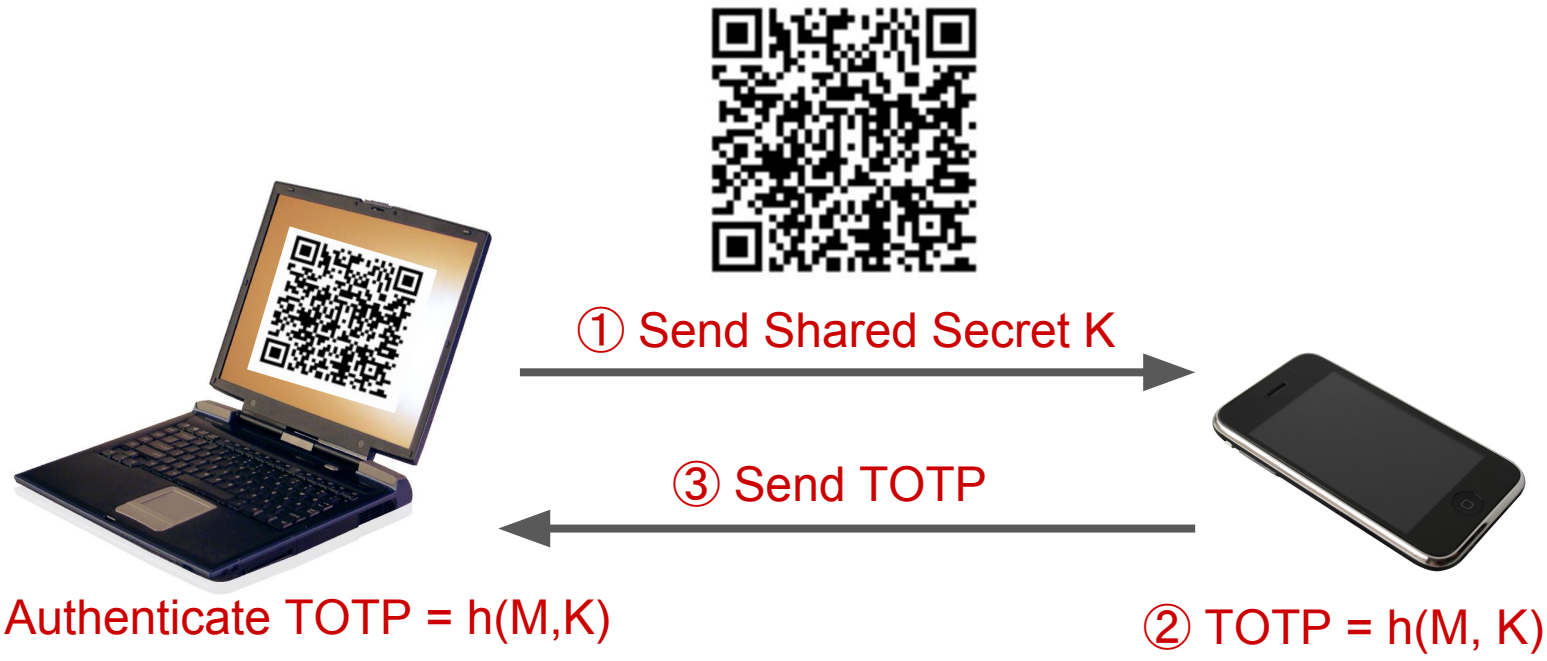
Websites with TOTP



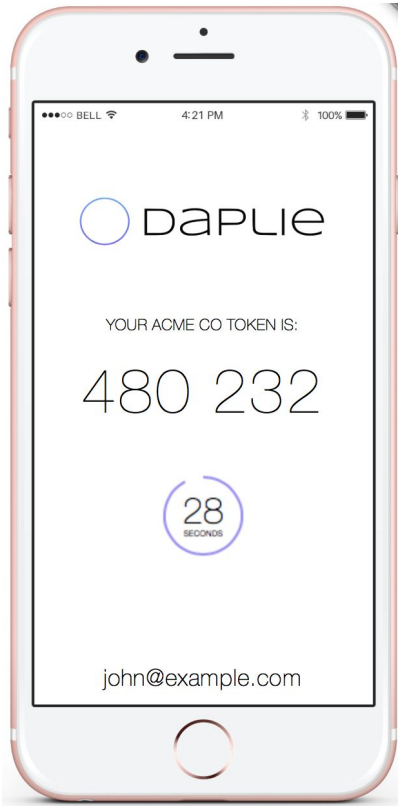
TOTP Algorithm: RFC standard 6238



Two Factor Authentication with TOTP Algorithm

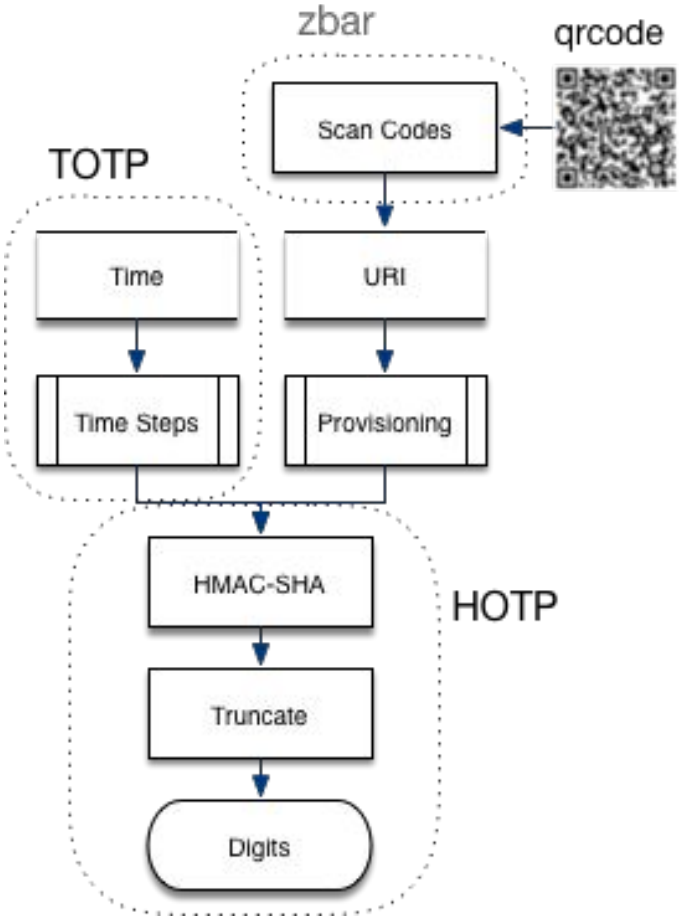


Setting Up TOTP on a Phone



pyOTP

- Implemented in Python 3 with zbar image processing library
- Available at **github.com/colematt/pyOTP**
- Compact and lightweight!
  - Library is 150 LOC
  - Demo is 144 LOC



Assessment of TOTP

- Proven Secure
  - Observing any number of past TOTP values cannot predict the next TOTP value
  - Most effective attack is *brute force*
- Some Attacks Are Still Possible
  - Replay within a time step -- mitigated by SSL
  - QR code stealing
- What if my device is stolen (TOTP is “Something You Have”)
  - … but that’s no worse than 1FA