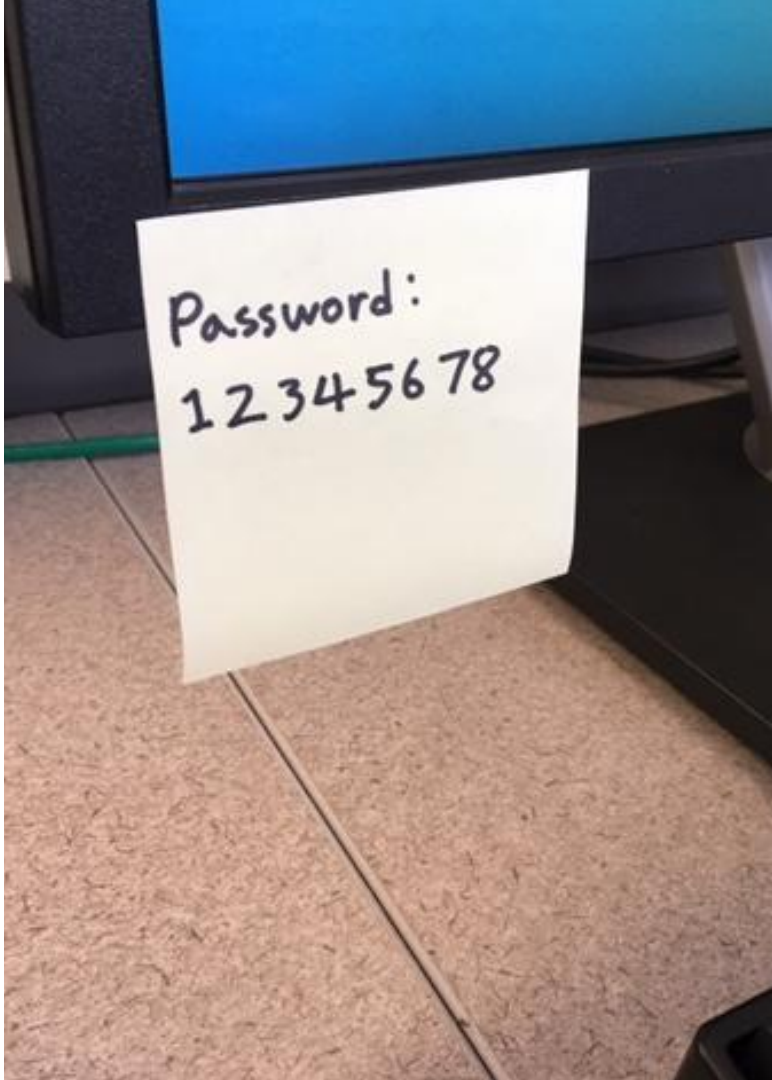
Time-Based One-Time Password Algorithm

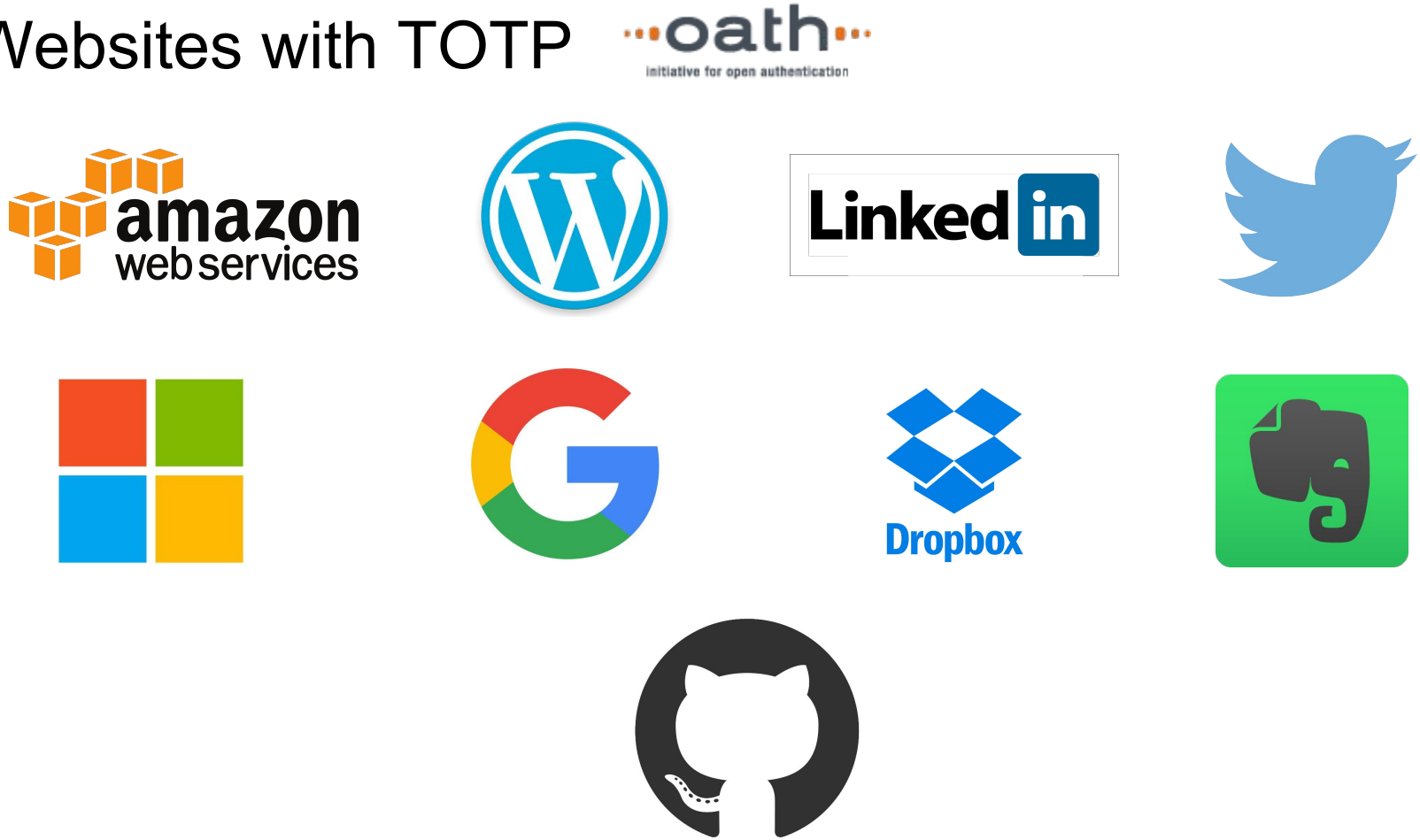
Matthew Cole, Anh Quach, Daniel Townley

Introducing TOTP

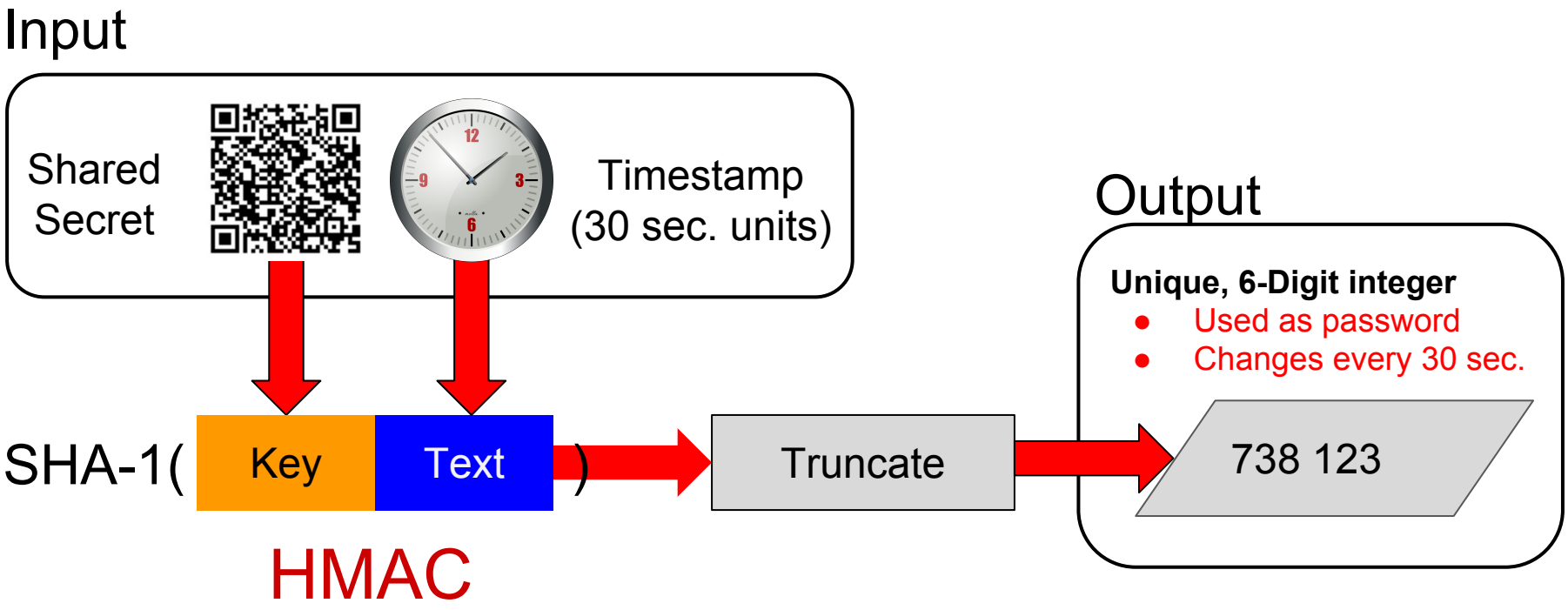
- Problem: password-based authentication invites replay attacks
- Defense: change password regularly
  - Sans Institute recommends every 3 months
  - Encourages weak passwords
  - Still enough time for replay attacks
- Can we change the password *every 30 seconds?*
  - Not as crazy as it sounds...



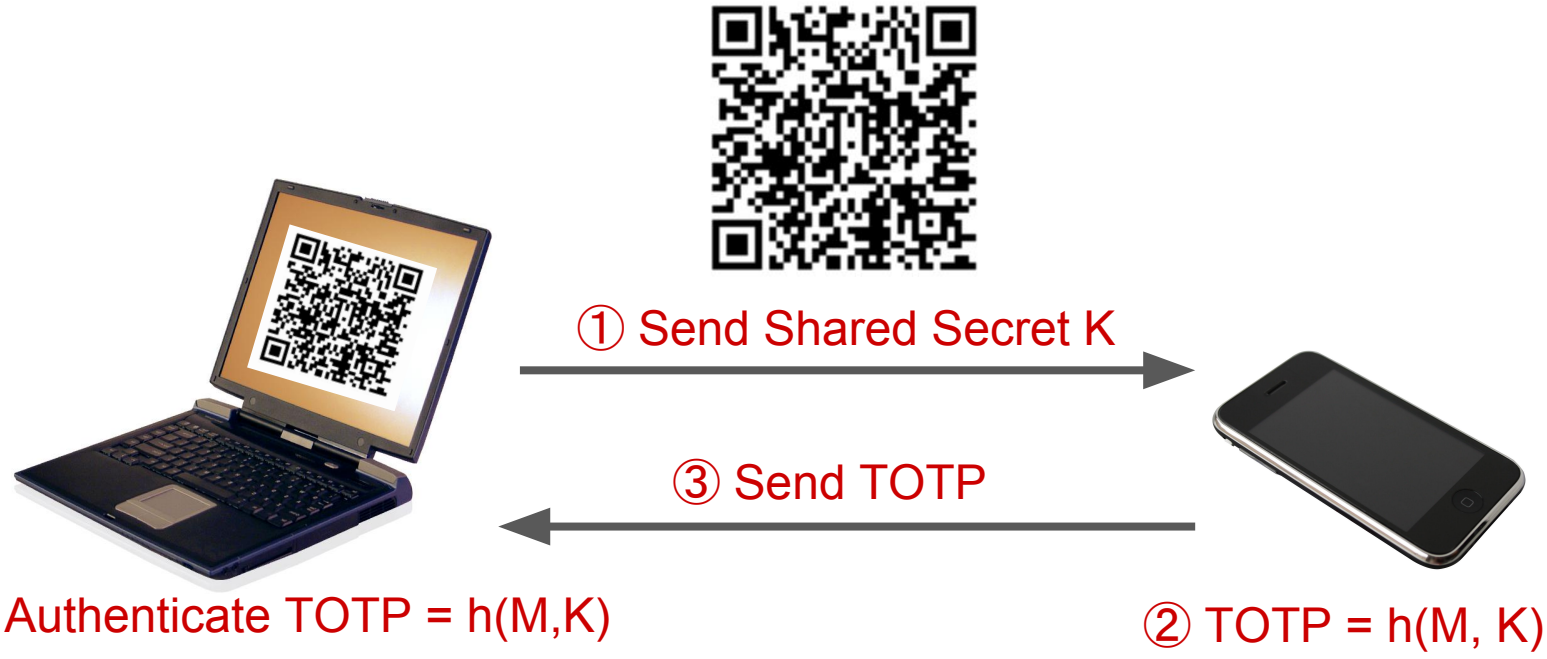
Websites with TOTP



TOTP Algorithm: RFC standard 6238



Authentication with TOTP Algorithm



Scan These

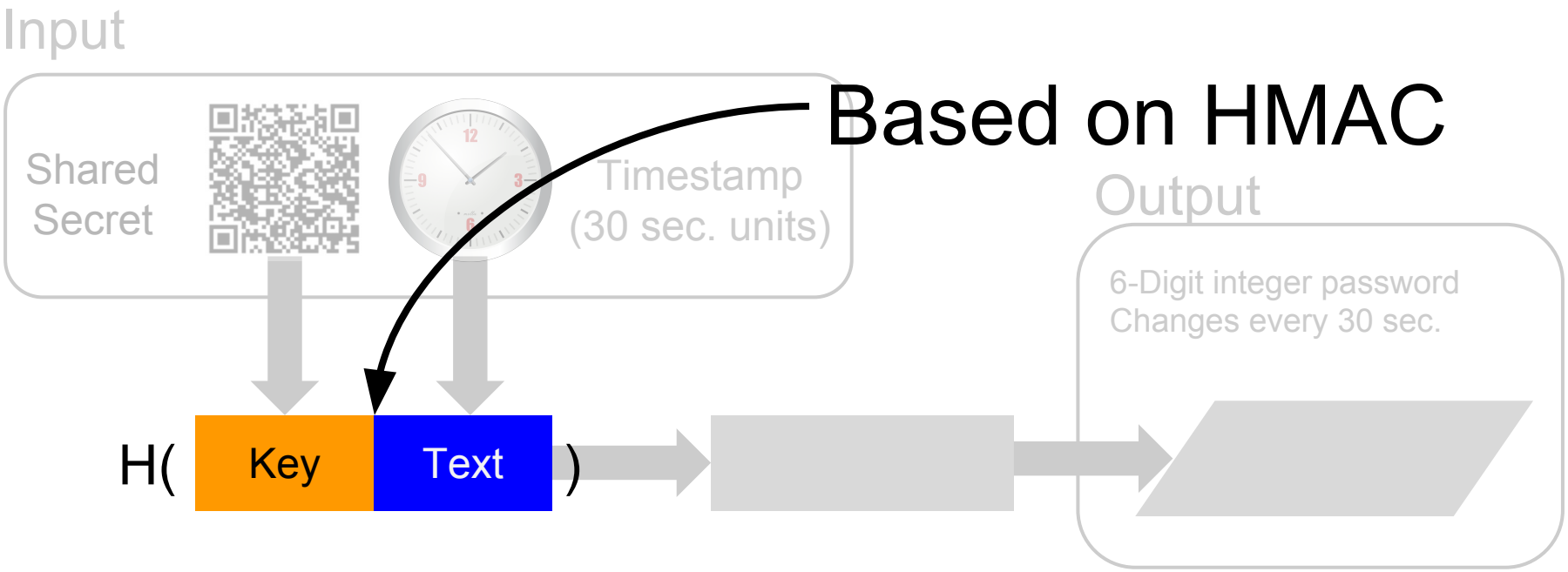
Android

iOS

Assessment of TOTP

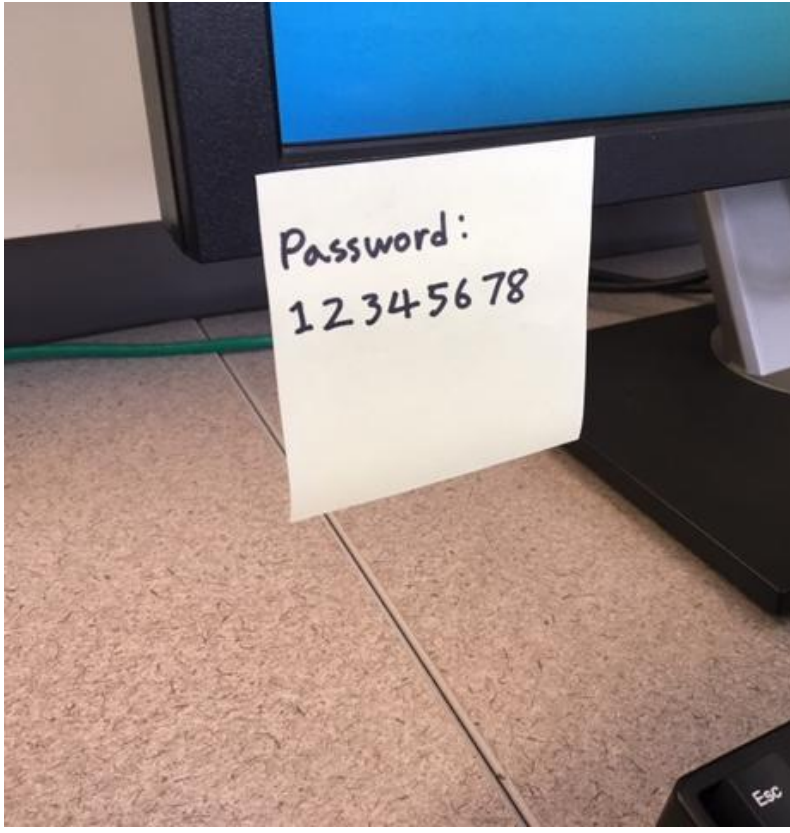
- Proven Secure
  - TOTP strength depends on HOTP
  - HOTP is proven secure
- Attacks only possible if implemented incorrectly:
  - Brute force
  - Replay
  - QR code stealing
  - Device stealing (TOTP is “Something You Have”)

TOTP Algorithm: RFC standard 6238



Dealing with Vulnerable Passwords

- Change compromised passwords?
  - But how to detect when they are compromised?
- Change Passwords every few months?
  - Recommended by Sans Institute
  - Difficult to maintain discipline
  - Enough time to launch attacks
- Change Passwords *every 30 seconds?*
  - Not as crazy as it sounds...



Time-Based One-Time Password Algorithm

- Based on HMAC protocol
  - Review: Residue of text M encrypted with key K
  - K is a shared secret
  - M is the current time
- Algorithm (RFC 6238)
  - K in units of 30 seconds
  - Take hash of K and M
  - Apply SHA-1 (yields very long number)
  - Truncate to 6-digit output
- Result: a new, unique password h(M, K) every 30 seconds