SECURE SYSTEMS DEMO DAY 2026 · USABLE SECURITY & PRIVACY

Tolerance for Errors in Authentication of Pervasive Services

M. Koistinen · S. Zuo · D. Mensah · E. Rhen · J. Taussi · M. Tiainen · N. Nevalainen · S. Tuominen · S. Sigg
Ambient Intelligent Group, Aalto University, Finland

Aalto University
School of Electrical
Engineering

THE PROBLEM

Why typos cost security

Passwords are the dominant means of authentication for pervasive services. Although strong ones impose a high cognitive load, they are hard to remember and to type. A frequent frustration is a login **rejected over a single minor typo.** Users react with security-degrading habits, such as reusing, shortening, or writing passwords down, leaving accounts open to dictionary attacks.

OUR APPROACH

Confidence-gated correction

Allow a limited number of typing errors, **but only when behavioural biometrics are confident it is really you.** That confidence comes from keystroke dynamics: a non-intrusive, software-only biometric. Because biometrics give convenience but not security (they can be observed and copied), we pair them with standard hashing, an error-correcting code repairs a confidence, limited number of symbols, then the result is checked against the stored password hash.

HOW IT WORKS

From keystroke to login

1. Enter credentials; a keystroke-dynamics sample is recorded while typing.
2. Server extracts features → biometric query, matched to the template → confidence ***c***.
3. Confidence ***c*** sets a Reed–Solomon budget ***t***; otherwise correction is skipped.
4. Repair up to ***t*** symbols, then run the normal password-hash check.

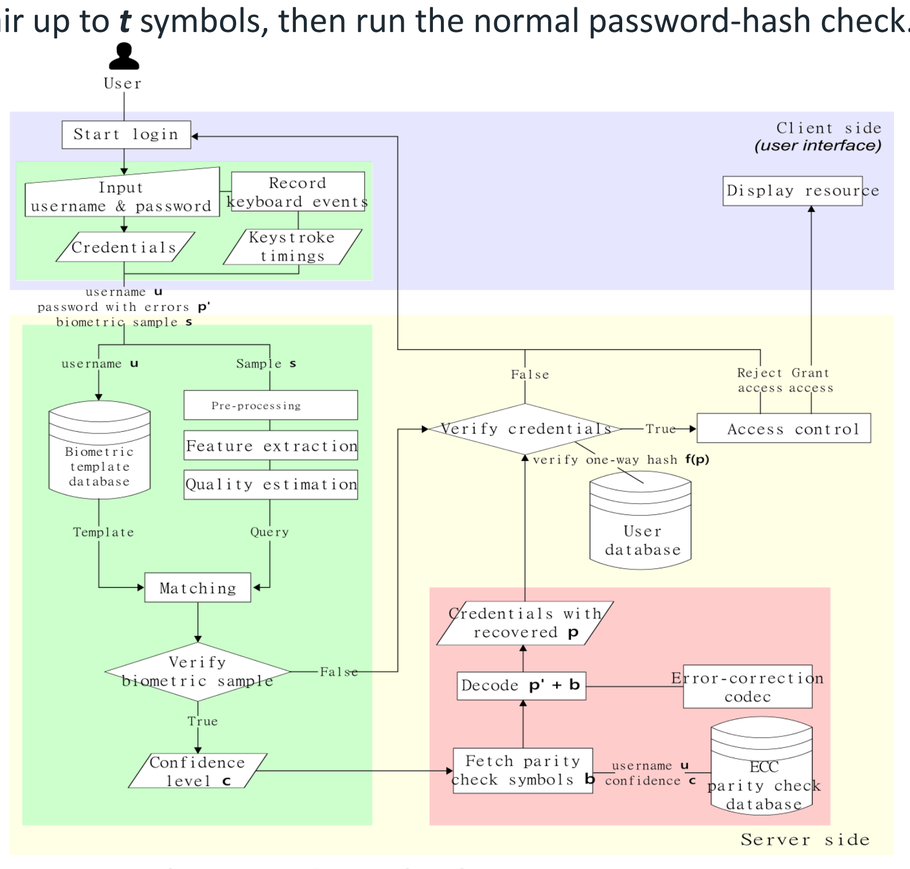


Figure 1: Keystroke dynamics features and Process flow for the proposed error-tolerant authentication system prototype. The client (purple) only records keystroke timing; the server verifies the keystroke biometric (green) and applies confidence-gated Reed–Solomon error-correction (red) before the ordinary one-way-hash check. Low confidence skips correction, leaving normal login unchanged.

KEYSTROKE DYNAMICS

Typing rhythm as a biometric

Everyone types with a habitual rhythm. From the password we extract **dwell-time, flight-time and intervals** into a timing vector. For a length-*n* password, that gives n dwell-times and *n−1* of each other feature. The vector is compared with a per-user template (the mean and standard deviation of recent samples).

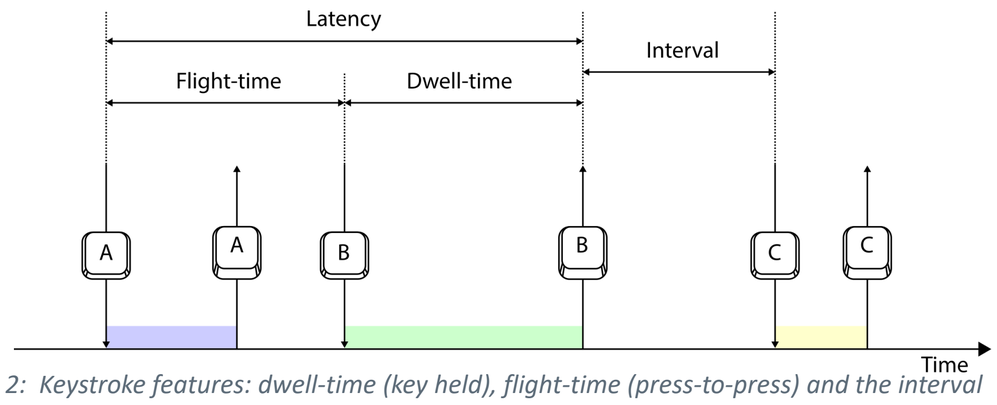


Figure 2: Keystroke features: dwell-time (key held), flight-time (press-to-press) and the interval between release and next press, from key-press / -release events.

Classifier	Equal Error Rate
Normalized Euclidean	24.62%
Gaussian distribution *best*	13.81%
Nonlinear	23.53%

Thresholds set at the Equal Error Rate; a sliding window of the 10 latest error-free samples adapts the template to drift.

ERROR CORRECTION

Reed–Solomon repair

Each password is encoded into Reed–Solomon code-words of increasing capacity t, and the biometric confidence selects which t to apply. Real typos are small: **88.9% of wrong passwords are within three edits** (Levenshtein), and 64.2% within three substitutions (Hamming). Correction cuts rejected logins by 42% at $t = 1$, 55% at $t = 2$ and 61% at $t = 3$.

SECURITY TRADE-OFF

Longer, stronger passwords

Correcting *k* of *n* symbols shrinks the password space from m^n to $C(n,k)\cdot m^{n-k}$, a small cost best reinvested in **length.** A 13-character password forgiving two typos matches the usability of a plain 7-character one, while being far stronger. Fuzzy cryptography stores hashes, not raw typing patterns.

CONCLUSION

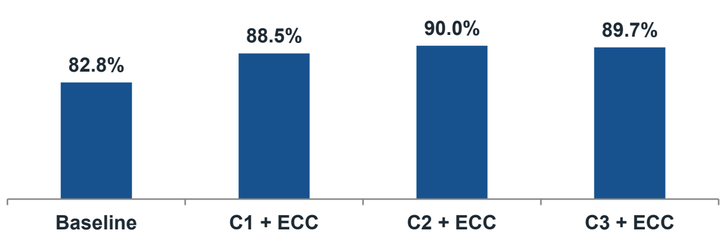
What it delivers

- Recovers about one third of rejected logins with no loss of security.
- Enables longer, stronger passwords at equal convenience.
- Extends to pattern-unlock; future work: multimodal confidence and password-drift correction.

RESULTS — 2,520 AUTHENTICATION EVENTS · 28 PARTICIPANTS · 7 DAYS

Login success rate

Successful logins rise from 82.8% to 90.0% (Gaussian + ECC).

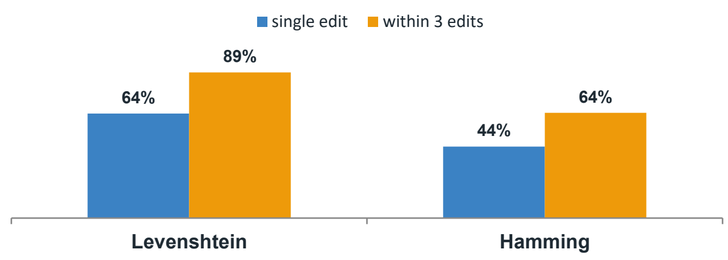


Fewer rejections as *t* grows

Rejected genuine logins drop as the budget t increases.

Error magnitudes

Typos repairable within one and within three edits.



Full paper