PRESS @$@$ TO LOGIN: STRONG WEARABLE SECOND FACTOR AUTHENTICATION VIA SHORT MEMORYWISE EFFORTLESS TYPING GESTURES

Prakash Shrestha*, Equifax Inc.
Nitesh Saxena*, Texas A&M University
Diksha Shukla+, University of Wyoming
Vir. V. Phoha, Syracuse University

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

* Work done at University of Alabama at Birmingham
+ Work done at Syracuse University

Syracuse University

Traditional One-time PIN based TFA (OTP-2FA)

Popular in web authentication

Traditional One-time PIN based TFA (OTP-2FA)

- Highly secure
- But, requires significant user-effort

Popular in web authentication

Traditional One-time PIN based TFA (OTP-2FA)

- Highly secure
- But, requires significant user-effort

What we want?

- Minimal-effort, yet secure, 2FA

Popular in web authentication

Emergence of Wearable 2FA

- 2FA variants are being rapidly gaining momentum on wrist-worn wearables: *Watch-2FA*
- Some examples
  - PIN-2FA: Google Auth and SAASPASS
  - Tap-2FA: Google Prompt, Duo Push
- Wrist-wearables are compelling platform for 2FA
  - Gaining popularity
  - Make 2FA easier for user compared to smartphone

Google Auth

SAASPASS

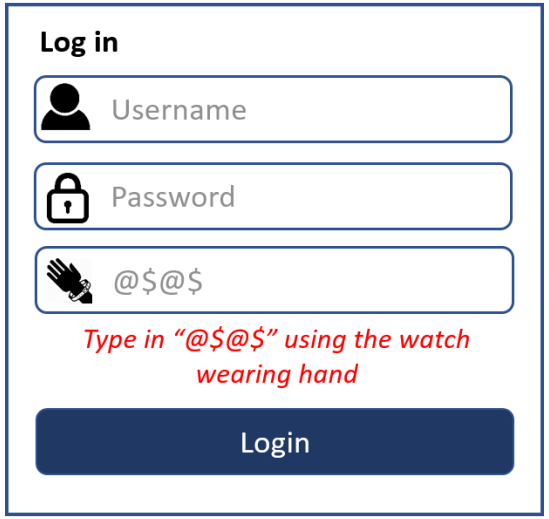
Google Prompt

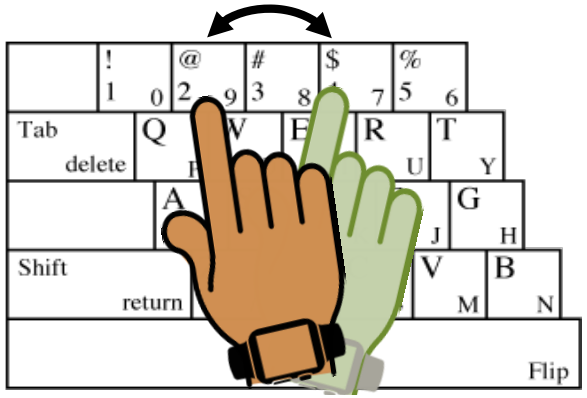
Duo Push

Fundamentals Problems with Current Deployments

- Require significant user-effort (PIN-2FA)
  - Interact with watch – launch app, read and copy OTP to authentication terminal
  - Divert user's attention away from authentication terminal
- Prone to user errors, negligence or click-through (Tap-2FA)
  - Small-form factor of watch make it difficult for user to view/read crucial login info
  - User is likely to accept or skip through login prompt
  - Susceptible to user negligence

Our Approach: SG-2FA



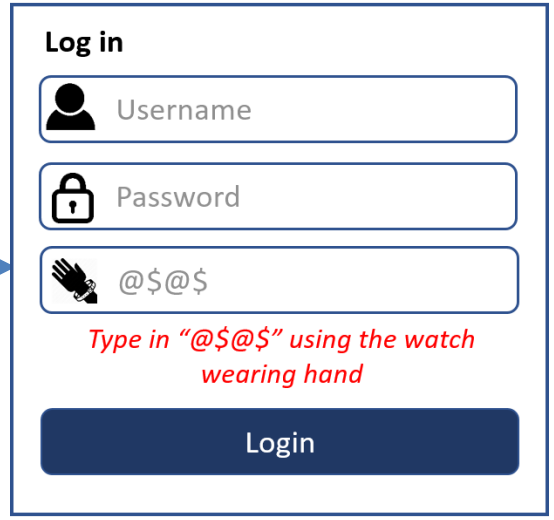


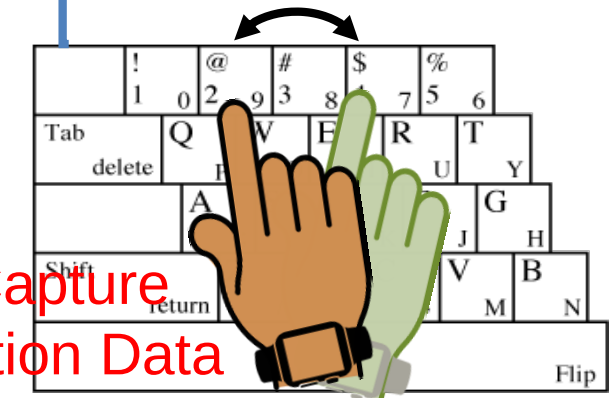
Smartwatch/Bracelet

Our Approach: SG-2FA

Provide credentials

& SCS (e.g., @$@$)

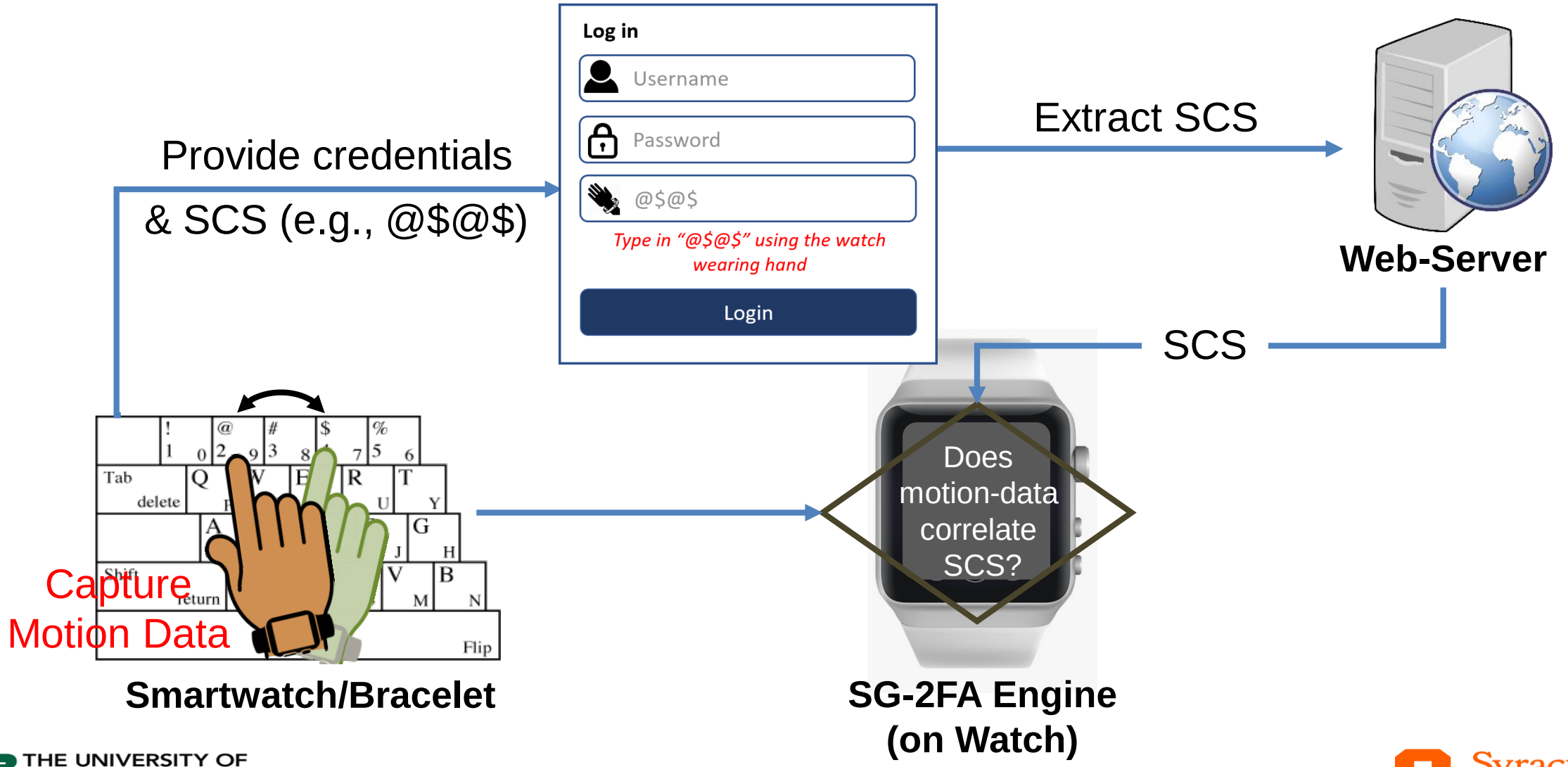




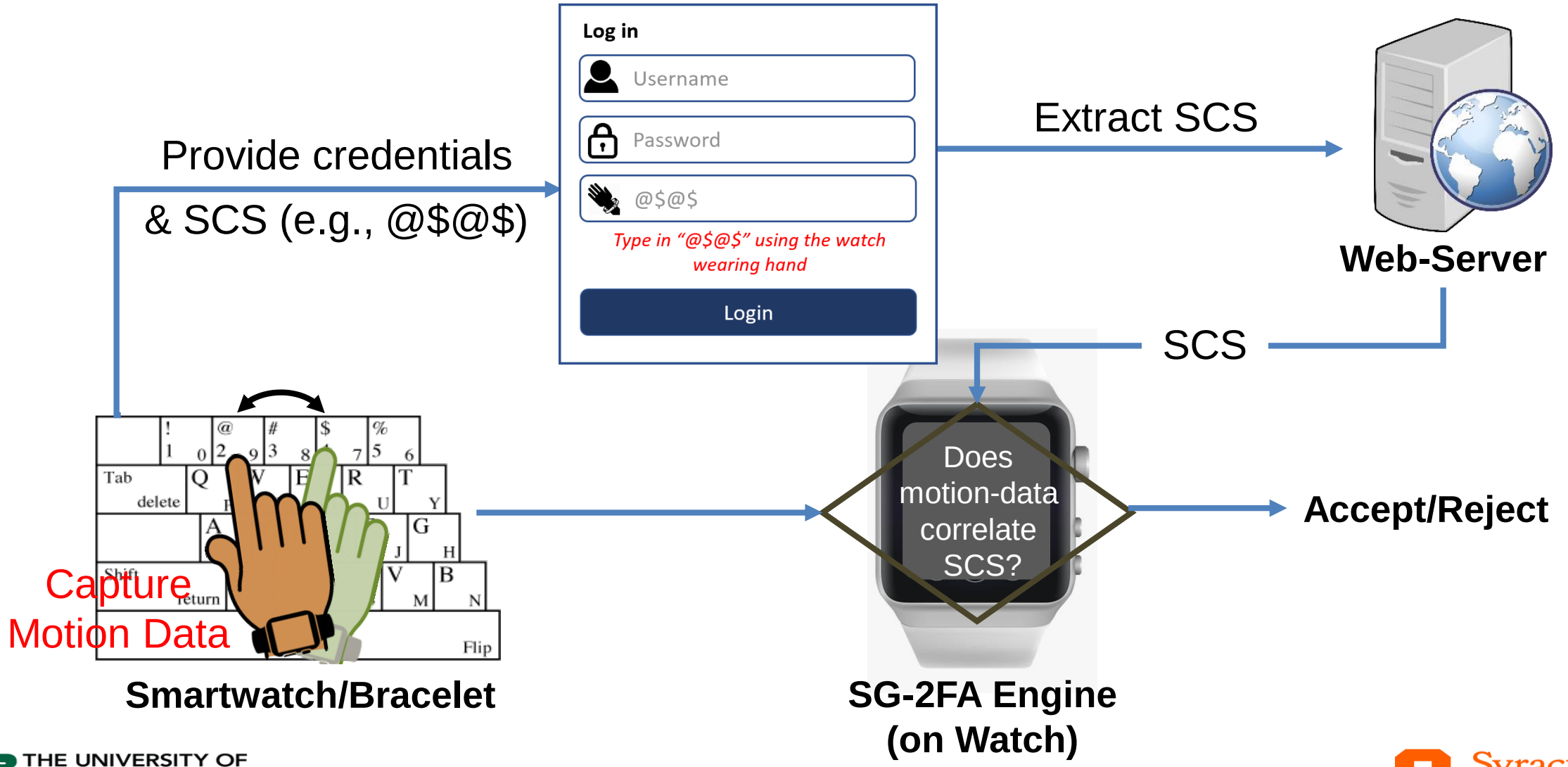
Capture Motion Data

Smartwatch/Bracelet

Our Approach: SG-2FA



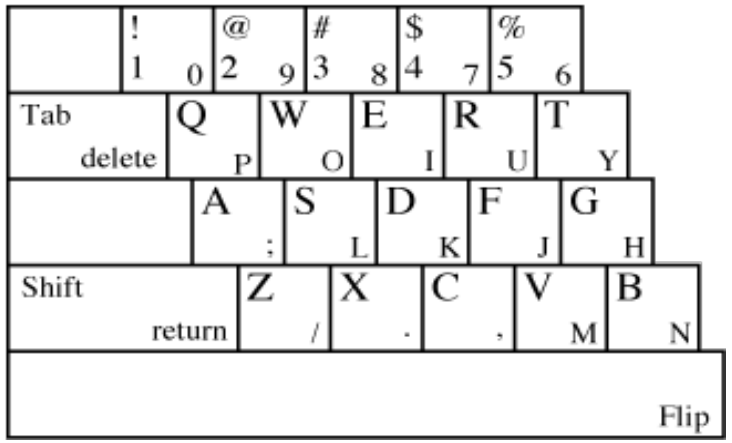
Our Approach: SG-2FA



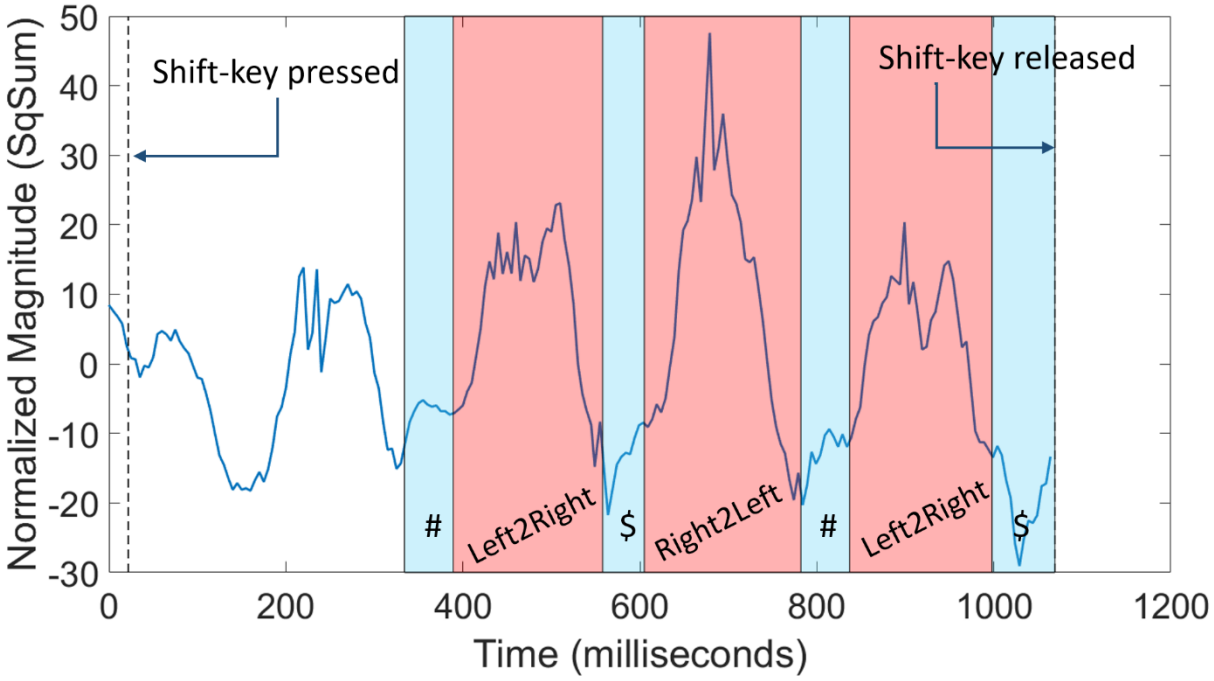
Special Character Sequence (SCS)

- Is formed using any *two different special characters* on the left side of standard QWERTY keyboard -- ~,!,@,#,$,%,^
- Special characters are *placed alternate to each other* that forces generation of unique wrist-motions – *left-to-right* or *right-to-left*
- Considered two parameters in our study
  - Length (len): number of characters in SCS (4, 5, 6)
  - Distance (dist): number of keys between two keys

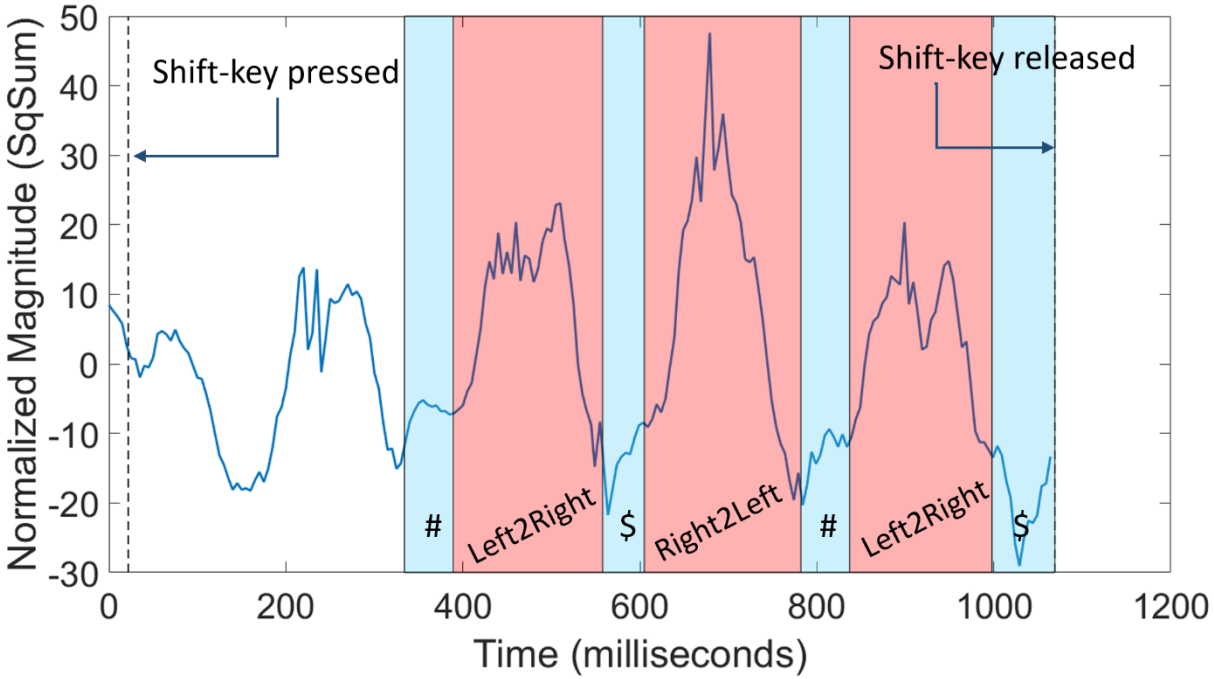
    e.g., for @$@$, distance = 1



Acceleration when typing “@$@$”



Acceleration when typing “@$@$”



Sequence of wrist-motions

Actual	L2R	R2L	L2R
Predicted	L2R	R2L	L2R

Our Contributions

- SG-2FA: Novel Wearable-2FA notion based on seamless gestures
- Design and implementation of SG-2FA
- Evaluation of SG-2FA in benign and adversarial settings

Threat Model and Attack Settings

- Adversary has gained victim user's login credential through phishing attacks, password database leakage, or other mechanisms
- Adversary cannot
  - gain physical access
  - compromise second factor device and victim's PC browser

Threat Model and Attack Settings

- Adversary has gained victim user's login credential through phishing attacks, password database leakage, or other mechanisms
- Adversary cannot
  - gain physical access
  - compromise second factor device and victim's PC browser
- We considered two potential classes of threats
  - Threat 1 – Regular Wrist Movements
    - User may perform everyday regular activities, e.g., walking, standing, resting on a chair, typing or playing game on a phone, etc., at the time of attack against SG-2FA
  - Threat 2 – Text Typing
    - User may be using computing device when at the time of attack against SG-2FA

Experiment Settings

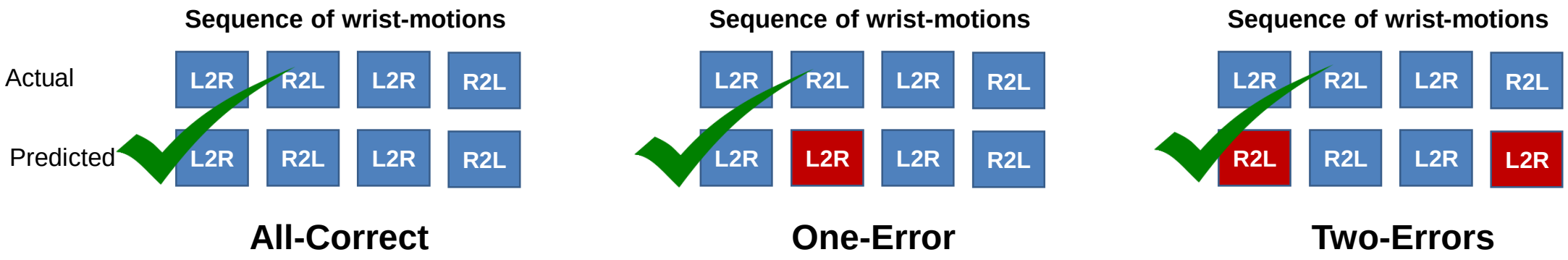
- Recruited 30 voluntary users at our University
- Participants chose 12 different types of SCS (3 SCS lengths and 4 key distances)
- They were asked to log in to our implementation of SG-2FA 10 times with each SCS created
- Repeated the experiment three times following 3x3 Latin square with time gap between (1-10) days
- Data samples for each of victim activities were also collected from randomly selected 2-5 participants

Evaluation Preliminaries: Performance Metrics

- Employed *Leave-One-Subject-Out (LOSO)* approach
  - For a given user, a classifier is built using samples from all other users.
  - Use of LOSO indicates model is **generic and user-agnostic**
- False Rejection Rate (FRR)
  - Rate of rejecting legitimate login
  - Used data instances when performing SCS-entries
- False Acceptance Rate (FAR)
  - Rate of accepting fraudulent login attempt
  - Used data instances when performing activities other than password-entry

Evaluation Preliminaries: Error Threshold

Error threshold: number of mis-predictions allowed



Results

Error-Threshold	SCS Length	FRR	FAR
One-Error	*Len3*	2.86	2.23
	Len4	4.47	0.45
	Len5	7.20	0.19
Two-Error	*Len5*	5.10	0.60

Results

Error-Threshold	SCS Length	FRR	FAR
One-Error	*Len3*	2.86	2.23
	Len4	4.47	0.45
	Len5	7.20	0.19
Two-Error	*Len5*	5.10	0.60

Results

Error-Threshold	SCS Length	FRR	FAR
One-Error	*Len3*	2.86	2.23
	Len4	4.47	0.45
	Len5	7.20	0.19
Two-Error	*Len5*	5.10	0.60

Limitations and Future Work

- Study with varying PCs
- Evaluate SG-2FA with large and diverse pool of users
- Evaluate SG-2FA with different laptop orientation
- Evaluate usability of SG-2FA vs. PIN-2FA and Tap-2FA

Conclusion

- Introduced low-effort wearable (watch-based) 2FA scheme based on the notion of seamless typing gestures -- SG-2FA
- Unlike PIN-2FA, SG-2FA
  - needs zero interaction with the watch
  - requires only a short sequence shown on the browser to be typed
- Compared to TAP-2FA, SG-2FA offers better security as there is no reliance on the user's decision making

Thank You!

Any Questions?