SaTC: TTP: Small: Collaborative: Privacy-Aware Wearable-Assisted Continuous Authentication Framework (NSF-CNS-1718116)

PIs: **A. Selcuk Uluagac**[1], **Kemal Akkaya**[1], **Koray Karabina**[2]
[1]Florida International University, [2]Florida Atlantic University
E-mail: [1]{suluagac, kakkaya}@fiu.edu, [2]kkarabina@fau.edu

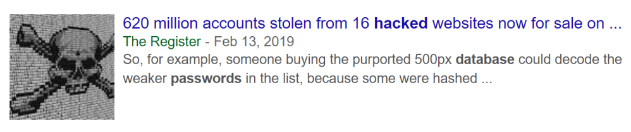
Abstract

One-time login process in conventional authentication systems does not guarantee that the identified user is the actual user throughout the session. Continuous authentication (CA), which re-verifies the user identity without breaking the continuity of the session, can address this issue. However, existing methods for CA are either not reliable or not usable. Moreover, These systems are increasingly coupled with other authentication factors such as biometrics in the authentication process to increase their usability. Nevertheless, biometrics systems demand more user information in their operations, yielding privacy issues for users in biometric-based authentication. In this paper, we introduce a usable, reliable, and privacy-preserving Wearable-Assisted Continuous Authentication (WACA) framework, which relies on the sensor-based keystroke dynamics and the authentication data is acquired through the built-in sensors of a wearable (e.g., smartwatch) while the user is typing. The empirical evaluation of WACA reveals that WACA is feasible, and its error rate is as low as 1% with 30 seconds of processing time and 2 - 3% for 20 seconds. Furthermore, WACA is capable of identifying insider threats with very high accuracy (99.2%) and also robust against powerful adversaries such as imitation and statistical attackers. Moreover, we also introduce a novel, secure, efficient, and privacy-aware continuous authentication protocol. Our system employs irreversible transformation on sensitive biometric user inputs, and does not rely on any trusted third party to provide privacy guarantees. It is built with encryption-free mechanisms for efficiency, and does not require any secret parameters, yet, it allows distinguishing genuine users from imposters even in noisy biometrics settings.

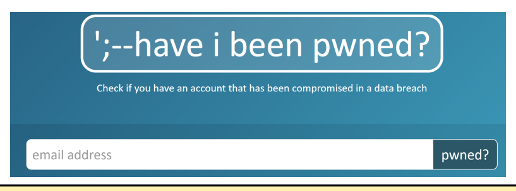
Authentication Problem

What the user knows	• Password, PIN, challenge-response
What the user has	• USB, smart card, key
What the user is	• Face, eye iris, DNA, fingerprint
How the user behaves	• Typing rhythm, gait, voice

- Passwords are most common, but password-only systems are subject to:
  - Social engineering attacks
  - Session hijacking
  - Insider attacks
  - Compromised database etc.



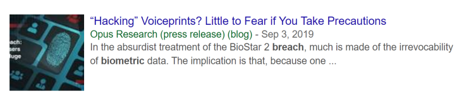
620 million accounts stolen from 16 **hacked** websites now for sale on ...
The Register - Feb 13, 2019
So, for example, someone buying the purported 500px **database** could decode the weaker **passwords** in the list, because some were hashed ...



';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?

Privacy Problem

- Biometrics increases the usability, but raises privacy concerns.

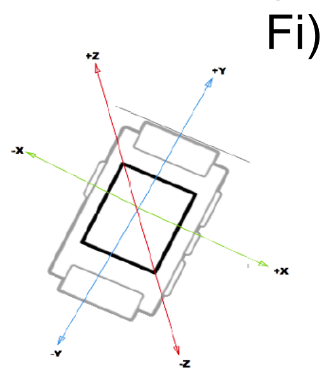


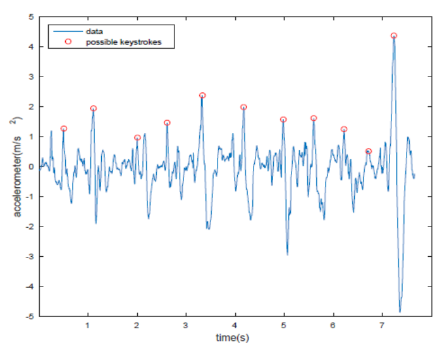
- The collected data for the purpose of enhancing security or other purposes raises serious privacy and security concerns for any smart environment equipped with smart devices.

- Even encrypted network traffic from a smart home environment can be used to infer sensitive information about smart devices and their users.

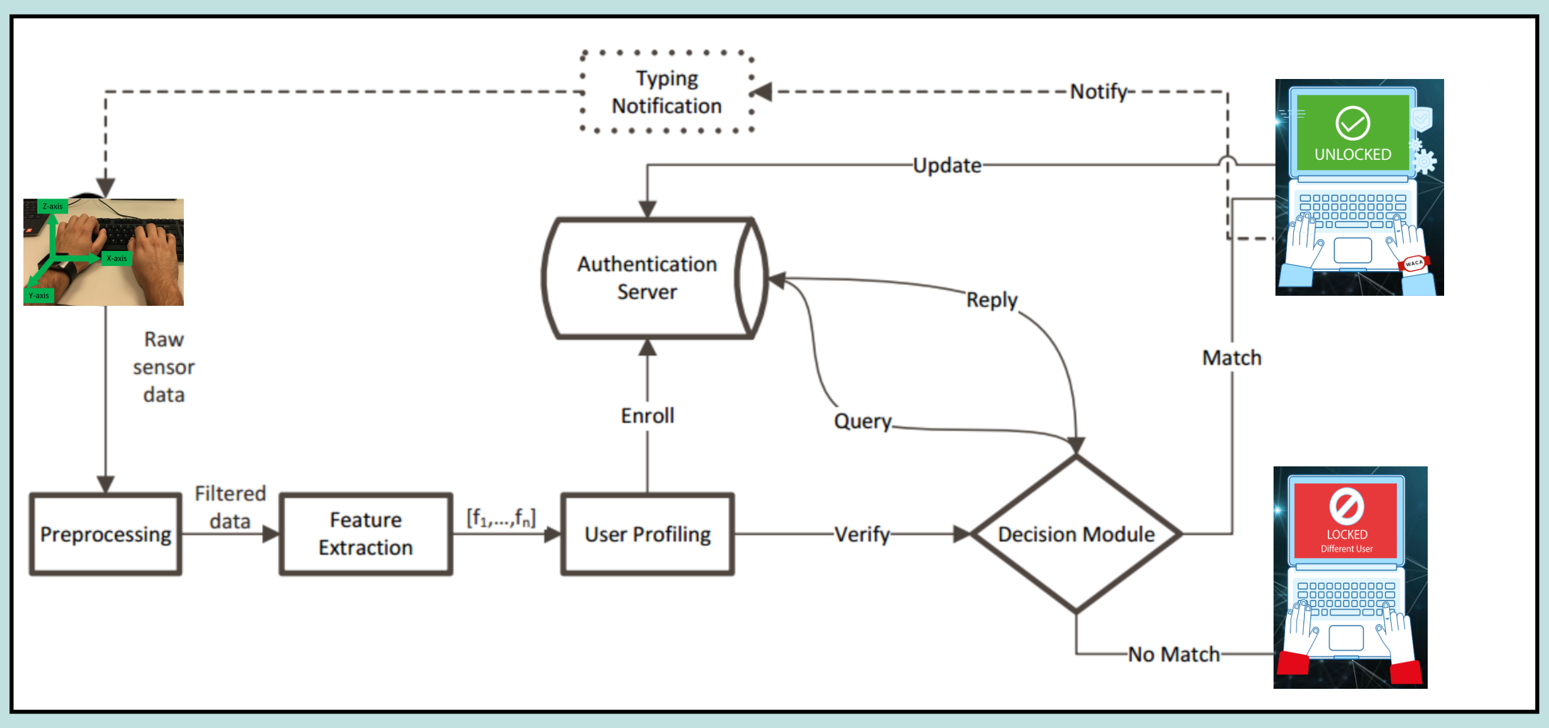
Wearables

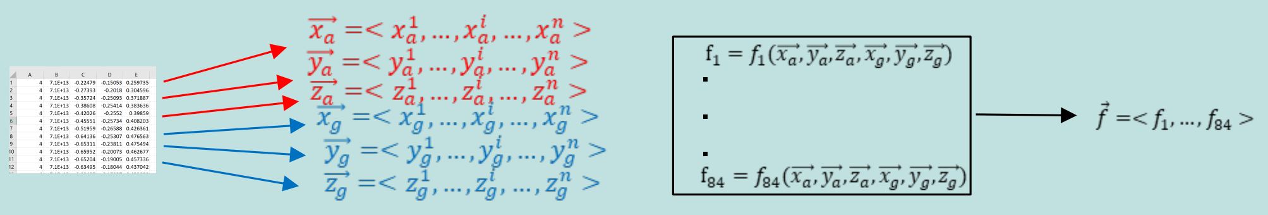
- Wearables have:
  - advance built-in sensors (e.g., accelerometer, GPS, thermometer, heart rate monitoring, etc.)
  - networking capability (e.g., Bluetooth and Wi-Fi)



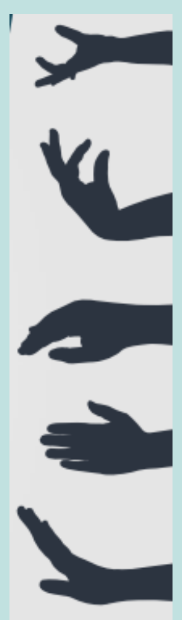


WACA Architecture



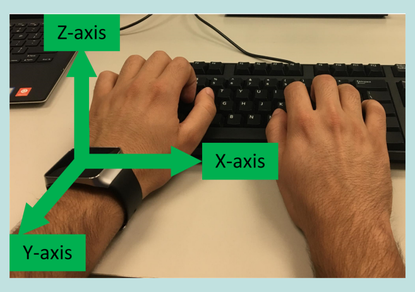

$\vec{x_a} =< x_a^1, \dots, x_a^i, \dots, x_a^n >$
$\vec{y_a} =< y_a^1, \dots, y_a^i, \dots, y_a^n >$
$\vec{z_a} =< z_a^1, \dots, z_a^i, \dots, z_a^n >$
$\vec{x_g} =< x_g^1, \dots, x_g^i, \dots, x_g^n >$
$\vec{y_g} =< y_g^1, \dots, y_g^i, \dots, y_g^n >$
$\vec{z_g} =< z_g^1, \dots, z_g^i, \dots, z_g^n >$
$f_1 = f_1(\vec{x_a}, \vec{y_a}, \vec{z_a}, \vec{x_g}, \vec{y_g}, \vec{z_g})$
$f_{84} = f_{84}(\vec{x_a}, \vec{y_a}, \vec{z_a}, \vec{x_g}, \vec{y_g}, \vec{z_g})$
$\vec{f} =< f_1, \dots, f_{84} >$

- Aim: Using the ubiquitous nature of wearables for the usability of continuous authentication.
- Key observation: Each person's wrist movements & actions are completely unique while typing.
- Collects data through smartwatch's motion sensors (i.e., accelerometer and gyroscope) keystroke dynamics from raw sensor data
- The feature vector (i.e., user profile) is created to profile the user
- Authentication using Distance Measure and Identification using Machine Learning Algorithms

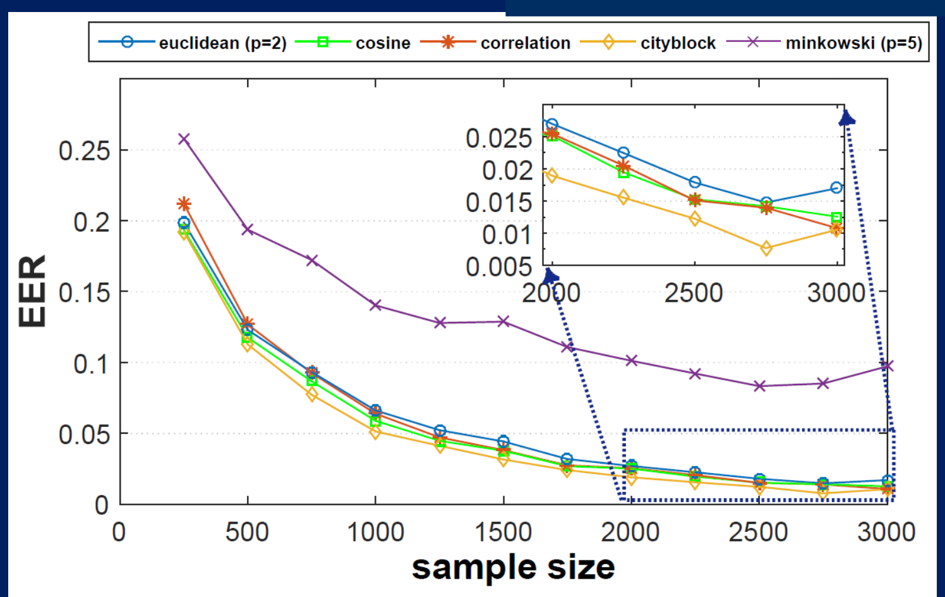


Experiments

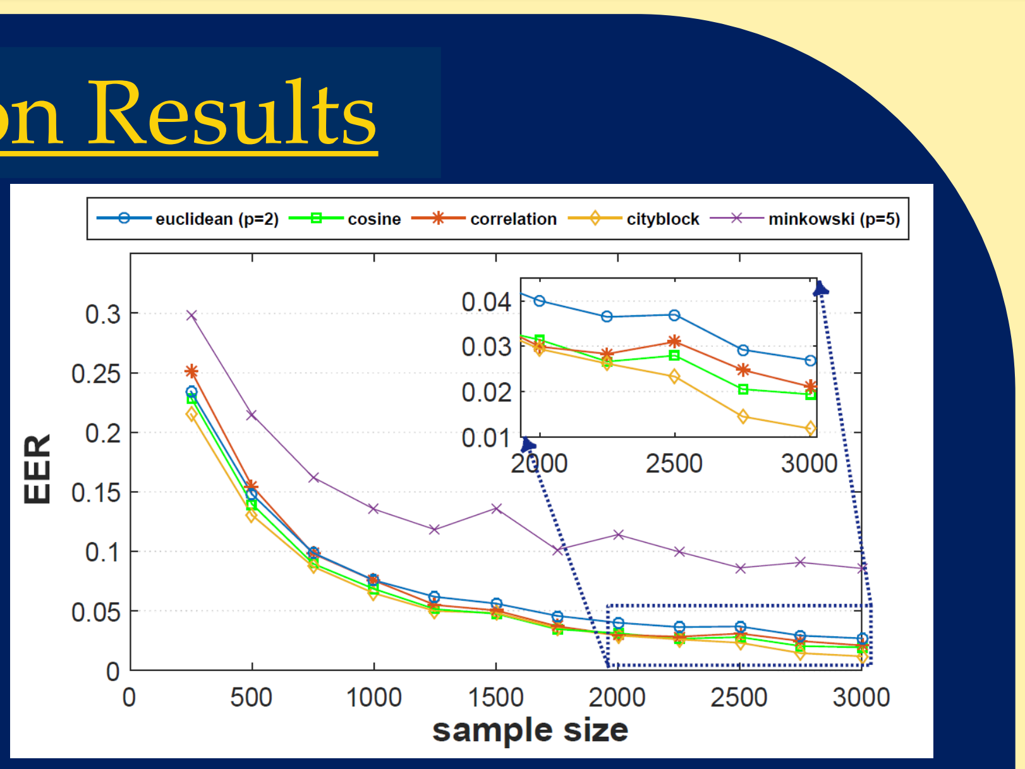
- **34 participants**
- LG G Watch R and Samsung Gear Live
- Android Wear app
- **6-axis motion** sensor(3-axis acc + 3-axis gyro)
- A **randomly selected** text and **same** text
- Qwerty keyboard



Authentication Results



a) Average EER according to different sample sizes using different distance metrics while users are performing Typing Task-1 (random-text).



b) Average EER according to different sample sizes using different distance metrics while users are performing Typing Task-2 (same-text).

Insider Threat Identification Results

Scenario 1: Accuracy (%)

	Training Set				
Sample size	1	2	3	4	5
1500	77.8	**93.7**	**97.2**	**98.4**	**99.2**
1000	62.8	87.6	**93.8**	**95.3**	**97.1**
500	37.5	63.7	75.9	83.1	89.6
250	28.5	43	53.1	61.8	62.1

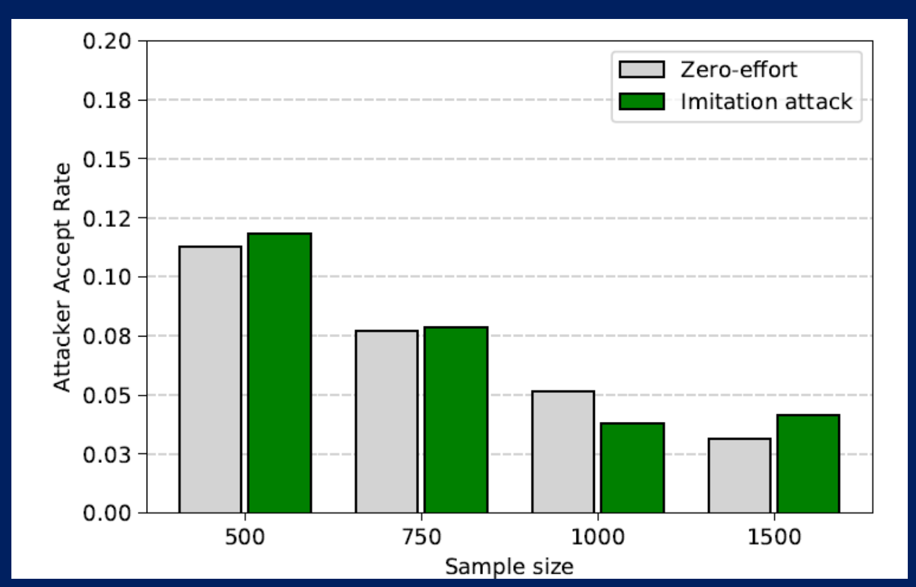
a) The accuracy results insider threat identification experiments for different sample sizes in Scenario 1.

Scenario 2: Accuracy (%)

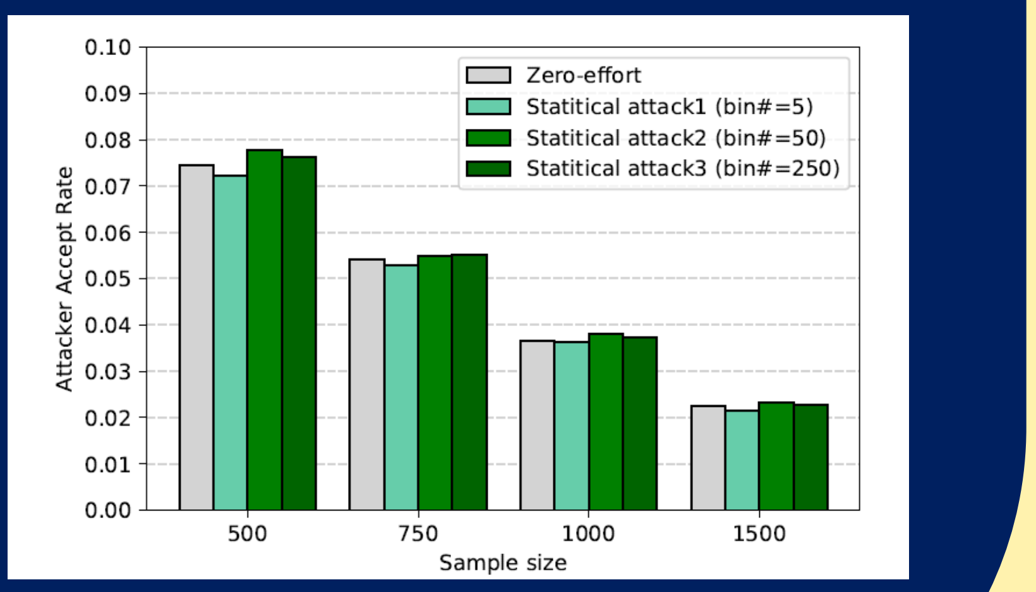
	Training Set				
Sample size	1	2	3	4	5
1500	55.8	80.1	88.7	89.8	**91.8**
1000	51.7	82.7	83.2	86.1	86.8
500	29.9	51.3	66.7	73.8	76.5
250	22.1	33.6	41.9	49.8	54.1

b) The accuracy results insider threat identification experiments for different sample sizes in Scenario 2.

Advanced Attacks on WACA

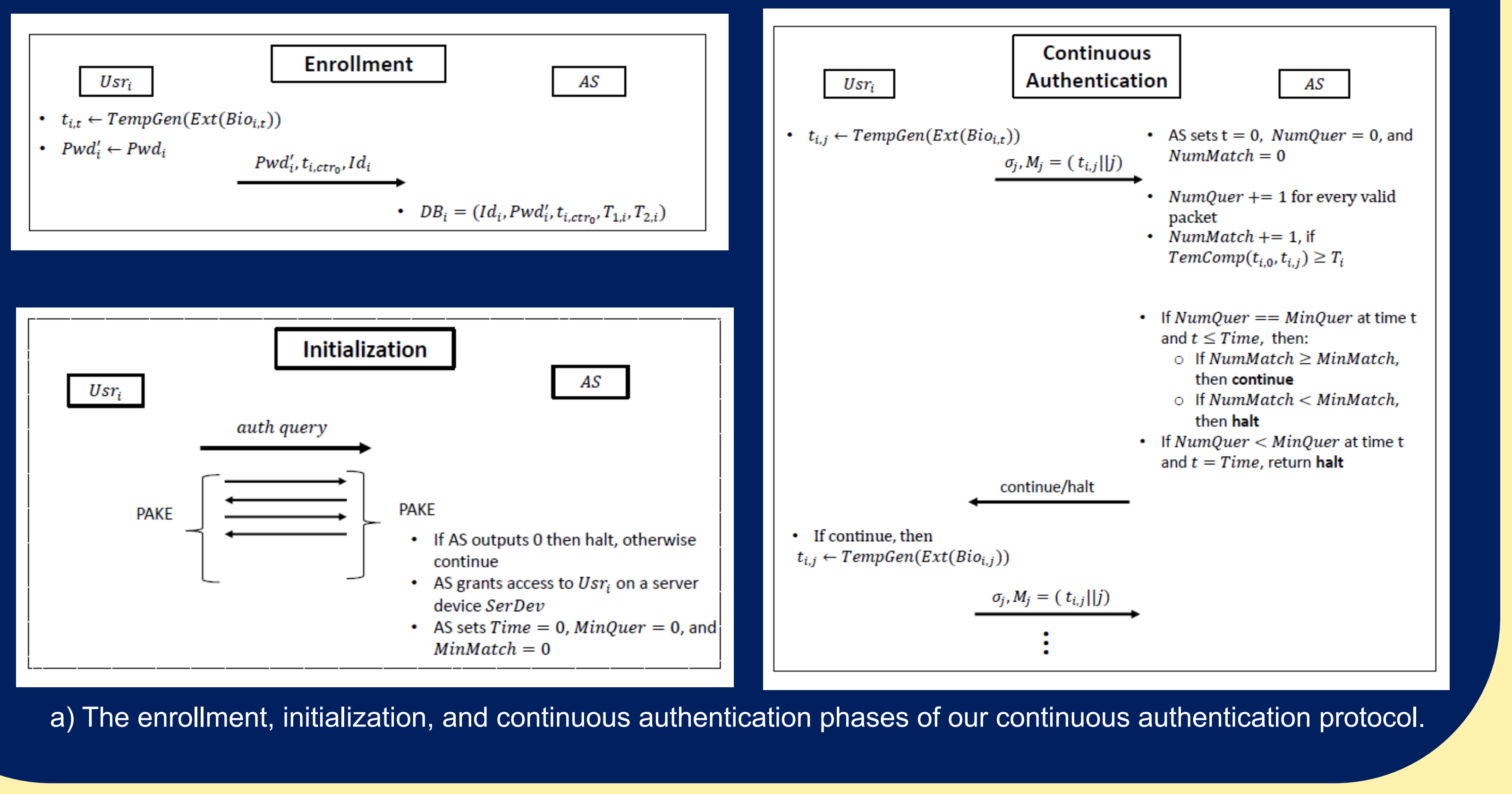


a) Attacker accept rates for different sample sizes. The results show that an imitation attacker has no more advantage than a zero-effort attacker.



b) 3 different statistical attacks against WACA with different sample sizes.

Privacy-aware Continuous Authentication Protocol



Enrollment

Usr_i | AS

- $t_{i,t} \leftarrow TempGen(Ext(Bio_{i,t}))$
- $Pwd_i' \leftarrow Pwd_i$

$\xrightarrow{Pwd_i', t_{i,ctr_0}, Id_i}$

- $DB_i = (Id_i, Pwd_i', t_{i,ctr_0}, T_{1,i}, T_{2,i})$

Initialization

Usr_i | AS

$\xrightarrow{auth\ query}$

PAKE | PAKE

- If AS outputs 0 then halt, otherwise continue
- AS grants access to Usr_i on a server device $SerDev$
- AS sets $Time = 0$, $MinQuer = 0$, and $MinMatch = 0$

Continuous Authentication

Usr_i | AS

- $t_{i,j} \leftarrow TempGen(Ext(Bio_{i,t}))$

$\xrightarrow{\sigma_j, M_j = (t_{i,j}||j)}$

- AS sets t = 0, $NumQuer = 0$, and $NumMatch = 0$
- $NumQuer$ += 1 for every valid packet
- $NumMatch$ += 1, if $TemComp(t_{i,0}, t_{i,j}) \geq T_i$
- If $NumQuer == MinQuer$ at time t and $t \leq Time$, then:
  - If $NumMatch \geq MinMatch$, then **continue**
  - If $NumMatch < MinMatch$, then **halt**
- If $NumQuer < MinQuer$ at time t and $t = Time$, return **halt**

continue/halt

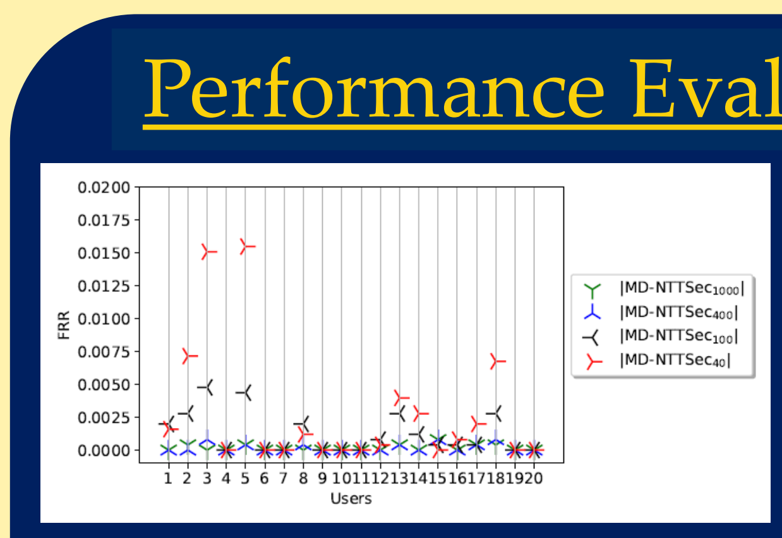
- If continue, then $t_{i,j} \leftarrow TempGen(Ext(Bio_{i,j}))$

$\xrightarrow{\sigma_j, M_j = (t_{i,j}||j)}$

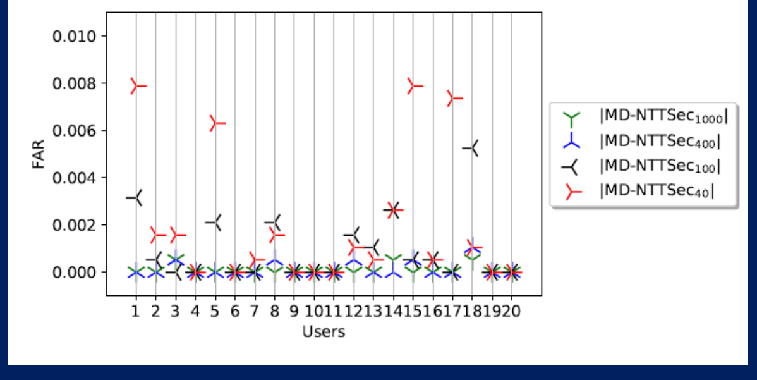
⋮

a) The enrollment, initialization, and continuous authentication phases of our continuous authentication protocol.

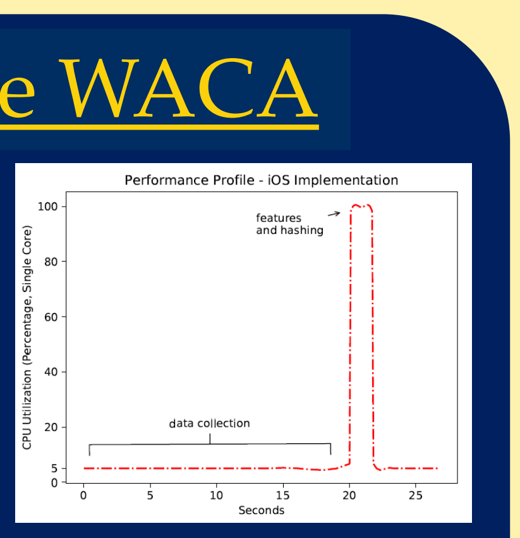
Performance Evaluation of Privacy-aware WACA



a) The absolute FRR difference between WACA and private-WACA implementations for all the 20 users.

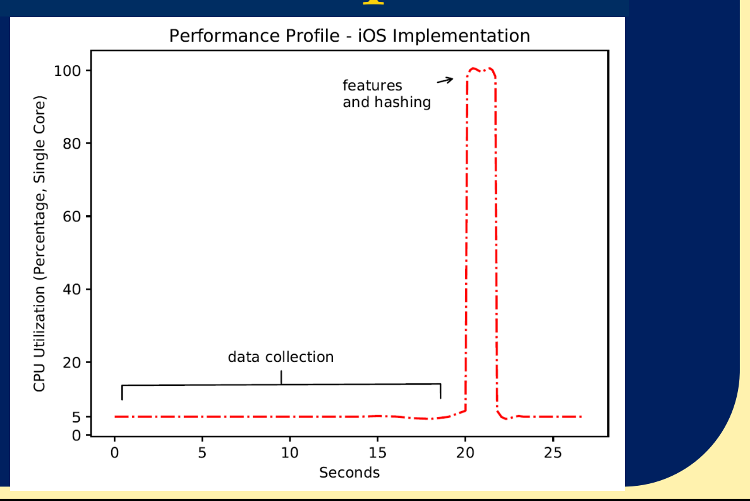


b) The absolute FAR difference between WACA and private-WACA implementations for all the 20 users.



c) Resource consumption of private-WACA implementation

Resource Consumption



References

1. Abbas Acar, Hidayet Aksu, Kemal Akkaya, and A. Selcuk Uluagac. WACA: Wearable-Assisted Continuous Authentication. In 39th IEEE Symposium on Security and Privacy Workshop, 2018.
2. Abbas Acar, Hidayet Aksu, Kemal Akkaya, and A. Selcuk Uluagac. WACA: Wearable-Assisted Continuous Authentication. In Transactions on Mobile Computing, 2018. (Under Review)
3. US Patent App. 15/674,133, "Method for continuous user authentication with wearables".
4. Abbas Acar, Wenyi Liu, Raheem Bayeh, Kemal Akkaya, and A. Selcuk Uluagac, "A Privacy-preserving Multi-factor Authentication System", Wiley Security and Privacy, 2019.

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

2019 SECURE AND TRUSTWORTHY CYBERSPACE PRINCIPAL INVESTIGATORS' MEETING (SATC PI MEETING '19)