May 13–17, 2024
Singapore, Singapore

Association for Computing Machinery

Advancing Computing as a Science & Profession

THE WEB CONFERENCE ACM

WWW '24 Companion

Companion Proceedings of the ACM Web Conference 2024

Sponsored by
ACM SIGWEB

General Chairs:
Tat-Seng Chua (National University of Singapore)
Chong-Wah Ngo (Singapore Management University)

Program Chairs:
Ravi Kumar (Google)
Hady W. Lauw (Singapore Management University)

Proceedings Chair:
Roy Ka-Wei Lee (Singapore University of Technology and Design)

One-shot Pairing and Authentication Using Moms Secret

Ubaid Ur Rehman
ubaid.rehman@khu.ac.kr
Kyung Hee University
Yongin-si, Gyeonggi-do, Korea

Sungyoung Lee
sylee@oslab.khu.ac.kr
Kyung Hee University
Yongin-si, Gyeonggi-do, Korea

ABSTRACT

The existing pairing and authentication mechanisms adopt either fuzzy commitment or fuzzy password-authenticated key exchange for device fingerprint generation, detecting and correcting multiple symbol errors, leading to guessing attacks and increased pairing time. In this study, we propose a one-shot pairing and authentication approach that generates a device fingerprint from the selected contextual data using Median-of-medians (Moms), ensuring randomness and preventing guessing attacks. Moreover, we integrate the Moms secret into Password Authenticated Key Exchange (PAKE) to reduce the pairing time and improve security. The evaluation demonstrates that our proposed one-shot pairing and authentication approach ensures strong resistance against information gain, reduces the probability of guessing attacks, and significantly decreases the pairing time compared to state-of-the-art approaches.

CCS CONCEPTS

• **Security and privacy** → **Authentication**; **Key management**.

KEYWORDS

Context, Pairing, Authentication, Moms Secret, Security

ACM Reference Format:
Ubaid Ur Rehman and Sungyoung Lee. 2024. One-shot Pairing and Authentication Using Moms Secret. In *Companion Proceedings of the ACM Web Conference 2024 (WWW '24 Companion), May 13–17, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3589335.3651542

1 INTRODUCTION

Pairing involves the establishment and computation of secret credentials (such as keys) among communication entities based on commonly sensed context [6]. Authentication, on the other hand, verifies and validates the identities of communicating entities. Our focus was on the identification of a single device or a group of devices based on their sensed contextual data. The recent trend in smart devices usually includes built-in onboard sensors that sense the surrounding environment and utilize the data for various services. According to our analysis, existing solutions are proposed in two major perspectives: user-centric [10] and device-centric [7]. User-centric approaches collect data associated with a specific user and ensure the authentication of devices in the user's possession. These approaches first identify user behavior based on collected data and initiate the pairing process to select legitimate devices in possession of the targeted user, preventing contextual co-presence attacks. In device-centric approaches, each device senses the surrounding environment and utilizes the collected data to identify legitimate devices within its proximity using pairing and authentication. The surrounding contextual data depend on the number of sensors involved in the data acquisition process and their corresponding data modalities; the collected data can be either single or multimodal [5].

In this study, we focus on how devices can mutually verify and validate their identity based on contextual data. We propose a one-shot pairing and authentication approach using Median-of-medians (Moms) secret generation for single and multimodal data. In a single modality, the Moms secret is generated using the device's physical context such as power consumption. Typically, the end device's contextual information is used by the centralized server to verify and validate its identity. It is assumed that the device's contextual data are already stored in a secure centralized repository and accessible to the server. The server acquires physical context of a specific device based on its identity, establishes a shared secret key, and identifies the end device based on the shared secret key. A prominent example is non-intrusive load monitoring data, where each appliance shares power consumption data with the centralized server for an energy management system. The goal of such pairing and authentication is to use physical contextual data as dynamic credentials, independent of time synchronization, reducing time complexity and computational overhead, and ensuring prevention against guessing attacks. In the case of pairing and authentication based on multimodal data, our proposed approach verifies and validates neighboring devices based on their ambient context, which supports personalized services in a smart environment. The objective is to reduce the computational overhead on the end devices for operating a separate communication protocol for authentication. Therefore, our proposed Moms secret generates the device fingerprint based on selected data dimensions from different modalities and uses it with Password Authenticated Key Exchange (PAKE) for shared secret key establishment. The key contributions of this study are as follows:

- We address the problem of time synchronization and low-entropy contextual information by proposing the Moms secret, which utilizes interval-based data that is independent of time synchronization and converts low-entropy values into high ones by taking the medians, ensuring randomness and preventing information leakage.
- We solve the problem of prolonged pairing time by selecting one data dimension from each modality based on similarity patterns. Then, we use the selected data dimension from all modalities for device fingerprint generation using the Moms secret. This significantly decreases predictability, increases entropy, and reduces pairing time.

WWW '24 Companion, May 13–17, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0172-6/24/05
https://doi.org/10.1145/3589335.3651542

- Existing approaches often adopt fuzzy-based methods for pairing and authentication, such as Reed-Solomon code, to detect and correct multiple symbol errors. However, adversaries can exploit this vulnerability to launch contextual co-presence attacks. To address this issue, we adopt PAKE and integrate it with the Moms secret, resulting in reduced pairing time and improved security.

2 ONE-SHOT PAIRING & AUTHENTICATION

The proposed one-shot pairing and authentication approach verifies and validates devices based on their single or multimodal contextual data. The contextual data may be physical, affiliated with the device, or ambient, sensed by the device. The term one-shot implies that only the end device's contextual information can be utilized by the verifier just once to perform pairing and authentication. Therefore, the attacker also has only one-shot to crack a specific session. The proposed approach acquires the contextual data, then generates a Moms secret, and finally establishes the key using PAKE. The detailed description of each step is described as follows.

2.1 Contextual Data Retrieval

The device shares its physical context with the centralized server for long-term storage, and the server can utilize the same interval of data for pairing and authentication. It is assumed that the physical context can be transmitted over a secure communication channel. The interval for selecting the context is predefined based on the number of instances. Each device's contextual data is linked with its unique identifier, which can be utilized while retrieving its corresponding context for validation and verification. Moreover, in the case of peer-to-peer pairing and authentication, each device needs to have the same type of sensing modules and environment to acquire the ambient context.

2.2 Moms Secret Generation

The device's physical context has low entropy, making it vulnerable to guessing attacks. Therefore, we propose a method to convert the low-entropy context value to high entropy using the Moms secret generation, as described in Algorithm 1. Initially, the selected time interval contextual data $(C_{t_1}, ..., C_{t_n})$ related to a specific device is acquired from the centralized repository based on the unique identifier of the targeted device. Then, compute the first median to divide the contextual data into two approximately equal size groups, denoted as $G_{f_{upper}}$ and $G_{f_{lower}}$. To convert the low-entropy value to high entropy, compute the median of $G_{f_{upper}}$ and $G_{f_{lower}}$ as s_{MedVal} and t_{MedVal}, respectively. Compare the corresponding groups ($G_{f_{upper}}$ and $G_{f_{lower}}$) with s_{MedVal} and t_{MedVal}, and store the resulting booleans in $G_{s_{upper}}$ and $G_{t_{lower}}$. To acquire the values in binary form, convert $G_{s_{upper}}$ and $G_{t_{lower}}$ into integers, resulting in zeros and ones, depicted as bits (G_{1bits} and G_{2bits}). Concatenate G_{1bits} and G_{2bits} into G_{concat} and convert it into bytes after padding (if required). Then reshape the G_{concat} into 8-bit chunks, convert it into string $S_{trChunk}$, and then decimal value $D_{ecChunk}$, formulating the elements ($Moms_{SecretElements}$) for Moms secret. Upon completion, the $Moms_{SecretElements}$ can be concatenated into sting $Moms_{SecStr}$ to make one value and then convert it to an integer to get our proposed Moms secret ($M_{oms_{secret}}$).

Algorithm 1: Moms Secret Generation

Input: Contextual data with respect to time $(C_{t_1}, ..., C_{t_n})$
Output: Generated Moms Secret $(M_{oms_{secret}})$

$d_{C_x} \leftarrow Collect(C_{t_1}, ..., C_{t_n})$ /* Contextual Data */
$f_{MedVal} \leftarrow median(d_{C_x})$ /* First Median */
$G_{f_{upper}} \leftarrow d_{C_x}[f_{MedVal} > d_{C_x}]$
$G_{f_{lower}} \leftarrow d_{C_x}[f_{MedVal} < d_{C_x}]$
$s_{MedVal} \leftarrow median(G_{f_{upper}})$ /* Second Median */
$G_{s_{upper}} \leftarrow s_{MedVal} \geq G_{f_{upper}}$
$t_{MedVal} \leftarrow median(G_{f_{lower}})$ /* Third Median */
$G_{t_{lower}} \leftarrow t_{MedVal} \leq G_{f_{lower}}$
$G_{1bits}, G_{2bits} \leftarrow int(G_{s_{upper}}), int(G_{t_{lower}})$
$G_{concat} \leftarrow G_{1bits} || G_{2bits}$
$P_{adBits} \leftarrow len(G_{concat})\ mod\ 8$ /* for bytes */
$P_{adBits} \leftarrow 8 - P_{adBits}$ /* Padding Bits */
if $P_{adBits} > 0$ **then**
  $G_{Pad} \leftarrow$ "0" $\times P_{adBits}$ /* Zero's Padding */
  $G_{concatPad} \leftarrow int(str(G_{concat}) + G_{Pad})$
else
  $G_{concatPad} \leftarrow G_{concat}$
$B_{itsChunk} \leftarrow$ reshape $G_{concatPad}$ into 8 *elements*
for *i in range*$(len(B_{itsChunk}))$ **do**
  $S_{trChunk} \leftarrow Concat_{Bits\_to\_Str}(B_{itsChunk}[i])$
  $D_{ecChunk} \leftarrow int(S_{trChunk}, 2)$
  $Moms_{SecretElements}.append(D_{ecChunk})$
$Moms_{SecStr} \leftarrow Concat_{Moms\_to\_Str}(Moms_{SecretElements})$
$M_{oms_{secret}} \leftarrow int(Moms_{SecStr})$

2.3 Moms Secret based on Multimodal and Multidimensional Contextual Data

According to our analysis, ambient contextual data is usually multimodal and multidimensional, including sensors such as accelerometer, gyroscope, and barometer, commonly used for context identification. Therefore, to generate the Moms secret from multimodal and multidimensional contextual data, the following steps are taken. Initially, the data from different modalities within the specified window size $(M_{1C_{t(ws)}}, ..., M_{nC_{t(ws)}})$ are loaded into a contextual modality dataframe ($\mathcal{M}Ctx$). The data dimension ($Mdims$) of each device's ambient context (c) retrieved from $\mathcal{M}_{Ctx}$ is assessed. In the case of uni-dimensional data, the $M_{omsSecret}$ is generated from the selected c as described in section 2.2 and appended with the multimodal-based Moms secret ($M_{ultiModalMoms_{Secret}}$). If the M_{dims} of a specific c has more than one data dimension, such as accelerometer and gyroscope, which have three dimensions, only one data dimension is selected based on the pre-defined rules. Then, the generated Moms secret is appended with the other sensors modalities in a pre-defined sequence.

2.4 Moms PAKE

PAKE presents the concept of establishing a shared secret key among communicating entities using a password known to the targeted devices [1]. PAKE relies on the concept of zero-knowledge

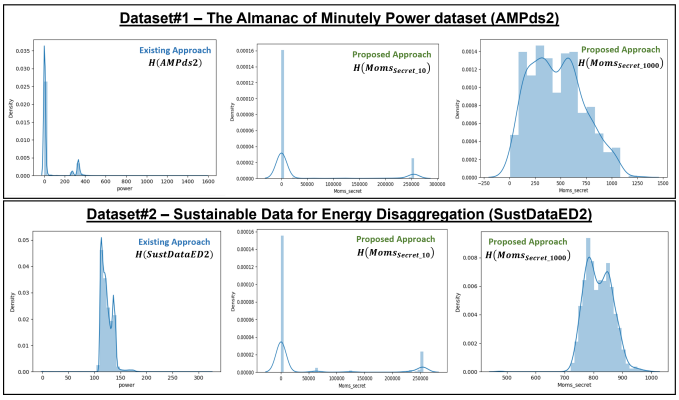

Figure 1: Shannon Entropy Assessment Between Existing (Ustundag et al. [13]) and Proposed One-shot Approach

proof, where devices can verify and validate the possession of a password without revealing or sharing it over the communication channel [2]. We use the generated $M_{oms_{secret}}$ or $M_{ultiModalMoms_{Secret}}$ as a device password ($D_{M_{oms_{secret}}}$) depending on the nature of contextual data and adopt PAKE to generate a 256-bit shared secret key for each device accordingly. Therefore, the security of our proposed one-shot pairing and authentication approach relies on the generation of Moms secret among the participating devices. In the case where the same symmetric key is generated on both devices, successful one-shot pairing and authentication occur. Otherwise, pairing and authentication fail.

3 EVALUATION AND RESULTS

The security of one-shot pairing and authentication depends on the acquired physical and ambient context, as well as the generated Moms secret. Therefore, we have evaluated our proposed approach based on three evaluation metrics, which include entropy assessment, probability of guessing attack, and pairing time. The acquired results for each evaluation criterion were compared with those of state-of-the-art approaches. The detailed description of dataset selection and evaluation metrics is provided below.

3.1 Dataset Selection

To evaluate our proposed one-shot pairing and authentication approach, we have selected datasets based on the contextual nature of the data.

3.1.1 Device Physical Context Datasets. We utilize the same datasets mentioned in [13] to reproduce their results and avoid bias. The first dataset is the Almanac of Minutely Power dataset (AMPds2), which contains data collected from a non-intrusive load monitoring system for two years and includes timestamps, voltage, current, and power as features [8]. The second dataset is the Sustainable Data for Energy Disaggregation (SustDataED2), which contains smart meter data attached to 18 appliances within one household [11].

3.1.2 Device Ambient Context Datasets. For the device ambient context dataset, we utilized co-presence-based pairing and authentication [4], [3]. Specifically, we selected the dataset related to the scenario involving cars, which was produced and used for the evaluation of FastZIP [3], similar to our proposed Moms PAKE. This dataset includes accelerometer (Acc), gyroscope (Gyr), and barometer (Bar) data collected from multiple smartphones placed in each car at various positions. The data collection encompasses both adversarial and non-adversarial settings.

3.2 Ablation Study for Multimodal and Multidimensional Moms Secret

To select an appropriate data dimension from multimodal and multidimensional contextual data, we conducted an ablation study on the FastZIP dataset [3], specifically for accelerometer (Acc) and gyroscope (Gyr), considering the x, y, and z data dimensions. We generated the Moms secret from each data dimension associated with the corresponding modalities and computed the similarity scores between the generated Moms secret. Our analysis on FastZIP data revealed the similarity percentages: 60.42% for (Acc_x, Acc_y), 50.24% for (Acc_x, Acc_z), 51.45% for (Acc_y, Acc_z), 52.21% for (Gyr_x, Gyr_y), 48.78% for (Gyr_x, Gyr_z), and 53.63% for (Gyr_y, Gyr_z). Thus, utilizing multidimensional data affiliated with the same modality would increase the computational overhead on end devices and lead to an unreliable Moms secret due to repeated bit patterns. Therefore, the correct Moms secret can be extracted using the dimensions (Acc_x, Gyr_z, Bar) on the FastZIP dataset.

3.3 Entropy Assessment

Entropy measures the state of disorder, randomness, and uncertainty in a given sequence. According to Claude Shannon [12], entropy is inversely proportional to information gain ($Entropy\ \alpha\ InformationGain^{-1}$). Therefore, we have computed the entropy of existing (Ustundag et al. [13]) and proposed one-shot approach using AMPds2 and SustDataED2 datasets, as shown in Figure 1. With the AMPds2 dataset, the entropy of the raw dataset used by existing approach is 2.1693, while the entropy of Moms secret with a small window size of 10 is 3.8805, and with a large window size of 1000 is 4.8454. In both cases, the entropy of our proposed approach is higher compared to the state-of-the-art. Similarly, for the SustDataED2 dataset, the entropy of existing approach is 3.1275, while the entropy of Moms secret generated with a window size of 10 instances is 3.8964, and with a window size of 1000 instances is 4.1728. These results indicate that the entropy of the Moms secret is higher compared to the Ustundag et al. scheme, suggesting that our proposed one-shot pairing and authentication mechanism ensures strong resistance against information gain and prevents predictive contextual attacks.

3.4 Probability of Guessing Attack

The probability of guessing attack indicate the likelihood of an attacker to guess a specific contextual value used for a specific operation. We have computed the probability of launching guessing attack on existing (Ustundag et al. [13]) and proposed approach using the AMPds2 and SustDataED2 datasets. The results shows that the probability of guessing Moms secret is less than guessing the physical context of devices used by the existing approach. Because Moms secret require to first guess the length of selected time interval, then identify the exact pattern and value on each position

that makes it hard for the adversary to guessing the Moms secret within the acceptable pairing and authentication time.

3.5 Pairing Time Assessment

Pairing time is the time required for an end device to complete the pairing process from data collection to secret key establishment. We evaluated the pairing time of our proposed Moms PAKE approach and compare with the state-of-the-art schemes of Fomichev et al. [4], [3]. For a fair comparison, we used the FastZIP dataset, select the window size (w_s) for multimodal data acquisition, and used two Raspberry Pi 4 Model B for Pairing time assessment. We assess pairing among the communicating entities (Raspberry Pi devices) using multimodal data selected in w_s, and incrementally slide the window upon completion of pairing process for the targeted scheme, then compute the average pairing time. Figure 2 demonstrates that Moms PAKE significantly reduces pairing time compared to Fuzzy PAKE [3] and Fuzzy Commitment [4]. For single-modality pairing using Acc, Gyr, and Bar, an average reduction in pairing time of 4.83% (Fuzzy PAKE) and 41.39% (Fuzzy Commitment) is observed. Similarly, for dual modalities, there is an average reduction of 22.67% (Fuzzy PAKE) and 56.91% (Fuzzy Commitment), and for triple modalities, an average reduction of 16.22% (Fuzzy PAKE) and 57.53% (Fuzzy Commitment). The greater reduction in pairing time for Moms PAKE is attributed to selecting one data dimension from multidimensional data per modality, instead of considering all for secret key generation as utilized by the state-of-the-art.

4 RELATED WORK

We have analyzed existing literature related to pairing and authentication based on a device's contextual data, considering both physical and ambient aspects. According to our analysis, existing approaches often utilize low-entropy contextual data for pairing and authentication, which can be exploited by adversaries for launching predictive contextual attacks [13]. Therefore, it is crucial to collect a sufficient amount of contextual data to provide adequate security, resulting in prolonged pairing times. Thus, existing solutions face a trade-off among security, computational overhead, and pairing time [9], [3]. Additionally, physical contextual data are often used in keyed hash functions for authentication, which increases overhead on resource-constrained devices [13]. Moreover, verification of neighboring devices based on ambient context approaches often utilizes fuzzy commitment, incorporating error correction mechanisms such as Reed-Solomon (RS) code to detect and correct multiple symbol errors [3]. However, adversaries can exploit this feature to launch contextual co-presence attacks [9].

5 CONCLUSION

In this study, we proposed a one-shot pairing and authentication approach using the Moms secret, which converts low entropy to high entropy, resulting in low information gain. We integrated the Moms secret as a password in PAKE to improve security and reduce the overall pairing time. In the future, we will assess our proposed approach based on intra-device and inter-device pairing.

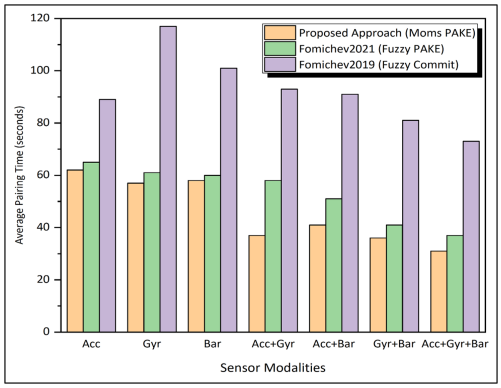

Figure 2: Pairing Time Reduction of Moms PAKE Compared to Fuzzy PAKE [3] and Fuzzy Commitment [4]

ACKNOWLEDGMENTS

This research was supported by the Korea Ministry of Science and ICT under the Grand ITRC support program (IITP-2022-2020-0-01489), the ITRC support program (RS-2023-00259004), (IITP-2022-0-00078, Explainable Logical Reasoning for Medical Knowledge Generation), and (IITP-2017-0-00655, Lean UX core technology and platform for any digital artifacts UX evaluation).

REFERENCES

[1] Michel Abdalla, Manuel Barbosa, Tatiana Bradley, Stanisław Jarecki, Jonathan Katz, and Jiayu Xu. 2020. Universally composable relaxed password authenticated key exchange. In *Annual International Cryptology Conference*. Springer, 278–307.
[2] Uriel Feige, Amos Fiat, and Adi Shamir. 1988. Zero-knowledge proofs of identity. *Journal of cryptology* 1, 2 (1988), 77–94.
[3] Mikhail Fomichev, Julia Hesse, Lars Almon, Timm Lippert, Jun Han, and Matthias Hollick. 2021. FastZIP: faster and more secure zero-interaction pairing. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. 440–452.
[4] Mikhail Fomichev, Max Maass, Lars Almon, Alejandro Molina, and Matthias Hollick. 2019. Perils of zero-interaction security in the Internet of Things. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 1 (2019), 1–38.
[5] Xiuwen Fu and Mingyuan Ren. 2024. Sustainable and Low-AoI Cooperative Data Acquisition in UAV-aided Sensor Networks. *IEEE Sensors Journal* (2024).
[6] Vivek Kumar, Sangram Ray, Dipanwita Sadhukhan, Jayashree Karmakar, and Mou Dasgupta. 2023. Enhanced pairing-free identity-based broadcast authentication protocol in WSN using ElGamal ECC. *Security and Privacy* 6, 3 (2023), e278.
[7] Khalid Mahmood, Salman Shamshad, Muhammad Faizan Ayub, Zahid Ghaffar, Muhammad Khurram Khan, and Ashok Kumar Das. 2023. Design of Provably Secure Authentication Protocol for Edge-Centric Maritime Transportation System. *IEEE Transactions on Intelligent Transportation Systems* (2023).
[8] Stephen Makonin. 2016. AMPds2: The Almanac of Minutely Power dataset (Version 2). https://doi.org/10.7910/DVN/FIE0S4
[9] Markus Miettinen, Nadarajah Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. 2014. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. 880–891.
[10] Rohini Poolat Parameswarath, Prosanta Gope, and Biplab Sikdar. 2023. Privacy-Preserving User-Centric Authentication Protocol for IoT-Enabled Vehicular Charging System Using Decentralized Identity. *IEEE Internet of Things Magazine* 6, 1 (2023), 70–75.
[11] Lucas Pereira, Donovan Costa, and Miguel Ribeiro. 2022. A residential labeled dataset for smart meter data analytics. *Scientific Data* 9, 1 (2022), 1–11.
[12] Claude Elwood Shannon. 1948. A mathematical theory of communication. *The Bell system technical journal* 27, 3 (1948), 379–423.
[13] Elif Ustundag Soykan, Leyli KaraÇay, Zeki Bilgin, Emrah Tomur, Mehmet Akif Ersoy, Ferhat KarakoÇ, and Pinar Çomak. 2021. Context-Aware Authentication with Dynamic Credentials using Electricity Consumption Data. *Comput. J.* (2021).