Proceedings of Second Shri Chhatrapati Shivaji Maharaj QIP Conference on Engineering Innovations
Organized by Shri Chhatrapati Shivaji Maharaj College of Engineering, Ahmednagar
In Association with Novateur Publications JournalNX-ISSN No: 2581-4230
February, 22nd and 23rd, 2019

Smartphone Sensor with App Data for Enhancing the Security of Secret Questions

Nikita Rave[1]
[1]Savitribai Phule Pune University,
Dept. of computer engineering, Shri Chhatrapati Shivaji Maharaj College of Engineering, Nepti, Ahmednagar, India
nikitarave22@gmail.com

Trupti Palkar[2]
[2]Savitribai Phule Pune University,
Dept. of computer engineering, Shri Chhatrapati Shivaji Maharaj College of Engineering, Nepti Ahmednagar, India
truptipalkar15@gmail.com

Punam Mote [3]
[3]Savitribai Phule Pune University,
Dept. of computer engineering, , Shri Chhatrapati Shivaji Maharaj College of Engineering, Nepti Ahmednagar, India
puns7890@gmail.com

Priyanka Alane[4]
[4]Savitribai Phule Pune University,
Dept. of computer engineering, Shri Chhatrapati Shivaji Maharaj College of Engineering, Nepti Ahmednagar, India
priyankaalane50@gmail.com

Under the Guidence of Prof

P.S Avhad

Abstract—At present with increasing popularity of online shopping Debit or Credit card fraud. Personal information security is major concerns for customers, merchants and banks specifically in the case of Card Not Present. Many web applications provide secondary authentication methods i.e., secret questions (or password recovery questions), to reset the account password when a user's login fails. Today's prevalence of smart phones has granted us new opportunities to observe and understand how the personal data collected by smart phone sensors and apps can help create personalized secret questions without violating the users' privacy concerns. We also provide a secure system for barcode-based visible light communication for online payment system using image stenography methodology. We present a Secret-Question based Authentication system, called "Secret- QA" that creates a set of secret questions on the basis of people's smart phone usage. We develop a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools meanwhile we observe the questions reliability by asking participants to answer their own questions.

Keywords— Security, Smartphone, Secret Question

I. INTRODUCTION (HEADING 1- TNR- 10 BOLD)

Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account password when a users login fails. However, the answers to many such secret questions can be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools (e.g., online social networks); moreover, a user may forget her/his answers long after creating the secret questions. Today's prevalence of smart phones has granted us new opportunities to observe and understand how the personal data collected by smart phone sensors and apps can help create personalized secret questions without violating the users privacy concerns. To developed a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools meanwhile we observe the questions reliability by asking participants to answer their own questions.

LITERATURE SURVEY

Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min Jerry Park, Xiaoming Li, Fan Ye, Wei Yan,

"Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions".

Many web applications provide secondary authentication methods, i.e., secret questions (or password recovery questions), to reset the account password when a users login fails. However, the answers to many such secret questions can be easily guessed by an acquaintance or exposed to a stranger that has access to public online tools (e.g., online social networks); moreover, a user may forget her/his answers long after creating the secret questions. Today's prevalence of smart phones has granted us new opportunities to observe and understand how the personal data collected by smart phone sensors and apps can help create personalized secret questions without violating the users privacy concerns. In this paper, we present a Secret- Question based Authentication system, called Secret-QA, that creates a set of secret questions on basic of people's smart phone usage. We develop a prototype on Android smart phones, and evaluate the security of the secret questions by asking the acquaintance/stranger who participate in our user study to guess the answers with and without the help of online tools; meanwhile, we observe the questions reliability by asking participants to answer their own questions. Our experimental results reveal that the secret questions related to motion sensors, calendar, app installment, and part of legacy app usage history (e.g., phone calls) have the best memorability for users as well as the highest robustness to attacks.

[1] **Wei-Han Lee and Ruby B. Lee, "Sensor-based Implicit Authentication of Smartphone Users".**

Authentication of smart phone users is important because a lot of sensitive data is stored in the smart phone and the smart phone is also used to access various cloud data and services. However, smart phones are easily stolen or co-opted by an attacker. Beyond the initial login, it is highly desirable to re-authenticate end- users who are continuing to access security critical services and data. Hence, this paper proposes a novel authentication system for implicit, continuous authentication of the smart phone user based on behavioral characteristics, by leveraging the sensors already ubiquitously built into smart phones. We propose novel context-based authentication models to differentiate the legitimate smart phone owner versus other users. We systematically show how to achieve high authentication accuracy with different design alternatives in sensor and feature selection, machine learning techniques, context detection and multiple devices. Our system can achieve excellent authentication performance with 98.1overhead and less than 2.4.

[2] **Stuart Schechter, Cormac Herley, Michael Mitzenmacher, "A New Approach To Protecting Passwords From Statistical-Guessing Attacks".**

We propose to strengthen user-selected passwords against statistical-guessing attacks by allowing users of Internet- scale systems to choose any password they want so long as it's not already too popular with other users. We create an oracle to identify undesirably popular passwords using an existing data structure known as a count-min sketch, which we populate with existing users' passwords and update with each new user password. Unlike most applications of probabilistic data structures, which seek to achieve only maximum acceptable rate false-positives, we set a minimum acceptable false-positive rate to confound attackers who might query the oracle or even obtain a copy of it.

[3] **Jong-hyuk Roh, Sung-Hun Lee, Soohyung Kim, "Keystroke Dynamics for Authentication in Smart Phone".** When entering a PIN on the touch screen of smart phone, users have their unique patterns, which shows different time interval, strength, position, and usage angel. Using this user's pattern, it is possible to distinguish the imposter who knows the users PIN, then the PIN verification can be enhanced in the smart phone environment. In this paper, we tested classifiers with five features that can be extracted from smart phone sensors. Also, we collected keystroke data for each user's posture, and compared the characteristics of the posture. We consider the importance of preprocessing and feature combinations.

[4] **Kai Li, Chau Yuen, Salil S. Kanhere, Kun Hu, Wei Zhang, Fan Jiang, Xiang Liu, "Understanding Crowd Density with A Smartphone Sensing System".**

In this paper, we demonstrate a proof-of-concept prototype of a lightweight indoor crowd monitoring system. The system utilizes off-the-shelf sensors which sniff probe requests periodically polled by people's smart phones in a passive manner. We propose a spatial -temporal data processing algorithm to study crowd density in a given area and their daily routine, based on a passive collection of the probe requests from their smart phones. Moreover, we carry out experiments to show the effect of the transmission interval of probe requests on the network traffic. We also undertake extensive experiments in real-world settings, i.e., one lab room in the university to observe office hours of researchers, and four closely located classrooms on the SUTD University campus to understand room occupancy.

II. PROPOSE SYSTEM

The reliability of a secret question is its memorability the required effort or difficulty of memorizing the correct answer. Without a careful choice of a blank filling secret question, a user may be declined to log in, because he cannot remember the exact answer that he provided, or he may misspell the input that requires the perfect literally-matching to the correct answer. We design a user authentication system with a set of secret questions created based on the data of user's short-term smart phone usage. We evaluated the reliability and security of the three types of secret questions (blank- filling, true/false, and multiple-choice) with a comprehensive experiment involving 88 participants. The experimental results show that the combination of multiple lightweight true-false and multiple choice questions required less input effort with the same strength provided by blank-filling questions. We evaluate the usability of the system, and find that the Secret-QA system is easier to use than those existing authentication system with secret questions based on user's long-term historic data.

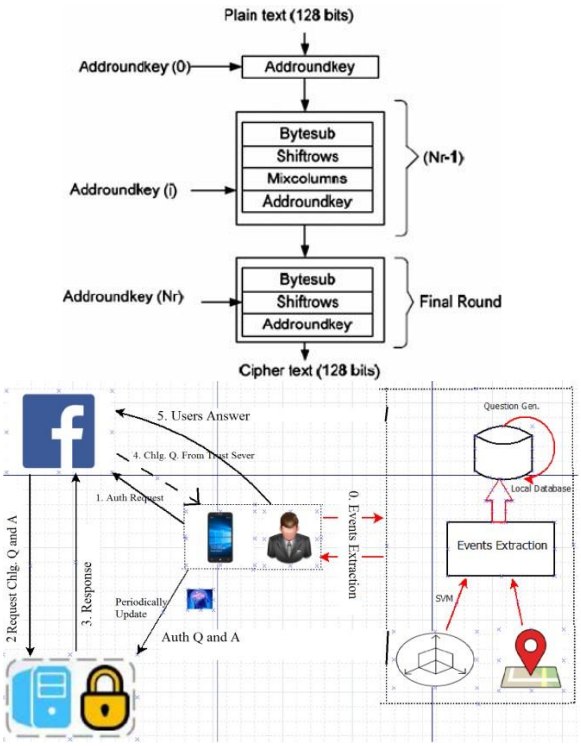
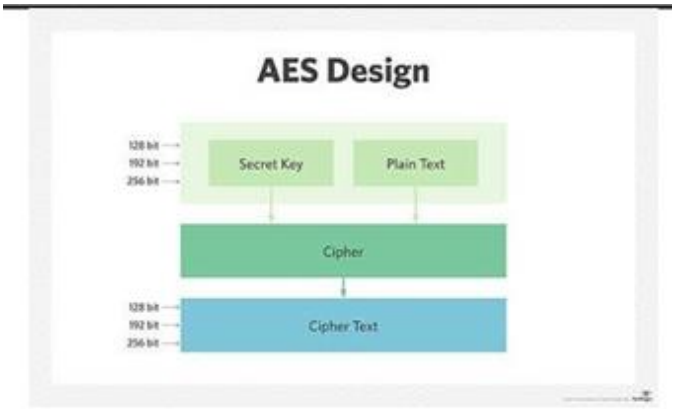


Fig 1: System Architecture

III. MODULES

1. The User-event Extraction Scheme
2. Participant Recruitment
3. Reliability and resilience to attacks
4. Report Generation
5. Secret Image Sharing

IV. ALGORITHM



for easier remembrance of user.

- The data of smart phone sensors and apps without violating the user privacy.

g 2: AES Design

Fig 3: Encryption Structure

V. MATHEMATICAL MODEL

Let S be the whole System, **S = {I, P, O}**

I = Input, P = Procedure, O = Output

I = {I0, I1, I2,I3}

I0 = Users activities (u1... un)

I1 = Event log (l1...ln)

I2 = Users answers (a1...an)

I3 = Users authentication request **P**

= {P0, P1, P2, P3}

P0 = Event Extract (e1...en)

P1 = Encryption phase

P2 = QA generation (qa1...qan)

P3 = Authentication request generation by user (Au1...Aun)

O = {O0, O1}

O0 = QA pair generated

O1 = User authentication

RESULT

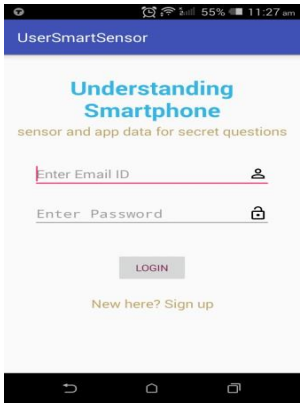


Fig 4: User Registration

VII. ADVANTAGES

The data of smart phone sensors and apps without violating the user privacy.

- In this Authentication system questions are True/false

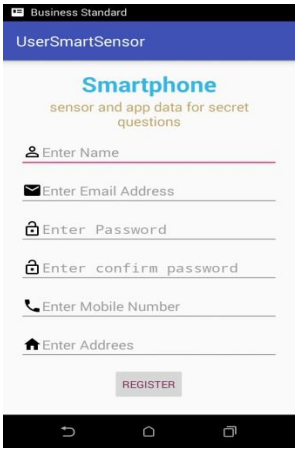


Fig 5: User Login

VIII. CONCLUSION

The secret questions related to motion sensors, calendar, app installment, and part of legacy apps (call) have the best performance in terms of memorability and the attack resilience, which outperform the conventional secret-question based approaches that are created based on a user's long-term history/information. In this system, our research provides a gridline that shows. Which sensors/app data and which type of question are suitable for devising secret question. This implies improved security for such secret questions.

IX. FUTURE SCOPE

In future work, we will try to adopt Wi-Fi or cellular location based service instead of GPS to further improve the battery life. Besides, the HTTPS traffic cost is almost negligible because our system will train and classify the motion related events locally, rather than sending the raw data of accelerometer/gyroscope to the server, and the root cause for HTTPS cost is the periodic update of secret questions/answers in an encrypted format.

References

[1] Peng Zhao, Kaigui Bian, Tong Zhao, Xintong Song, Jung-Min Jerry Park, Xiaoming Li, Fan Ye, Wei Yan, "Understanding Smartphone Sensor and App Data for Enhancing the Security of Secret Questions", IEEE, 2018.

[2] Wei-Han Lee and Ruby B. Lee, "Sensor-based Implicit Authentication of Smartphone Users", International Conference on Dependable Systems and Networks, 2017.

[3] Stuart Schechter, Cormac Herley, Michael Mitzenmacher, "A New Approach To Protecting Passwords From Statistical-Guessing Attacks", 2017.

[4] Jong-hyuk Roh, Sung-Hun Lee, Soohyung Kim, "Keystroke dynamics for authentication in smartphone", IEEE, 2016.

[5] Kai Li, Chau Yuen, Salil S. Kanhere, Kun Hu, Wei Zhang, Fan Jiang, Xiang Liu, "Understanding Crowd Density with A Smartphone Sensing System", 2016.