4

Review

I Know What You Did Last Week! Do You?: Dynamic Security Questions for Fallback Authentication on Smartphones

Technical Summary:

The authors [1] proposed an authentication scheme, which can be used once the user locks himself/herself out from his/her smartphone to regain the access. One of the traditional methods is to use Personal Unblocking Codes (PUC), but the issues with them that user can't carry them around. Additionally, if the user is in place where the internet connection or in a foreign country getting access to network operators to unblock the device or going to Google play or Apple online account becomes a tedious task. They used dynamic security questions which were based on the smartphones log on the user usage of SMS, app usage and various other parameters. They were able to determine which dynamic security question suits best to authentication schemes.

Contributions:

- Usable Design and Dynamic Security Questions: One of the main key ideas for this paper was the use of Personal Unlocking Codes when the duo factor authentication is exhausted by the adversary to access smartphone. To tackle this the proposed scheme of using dynamic security questions is one of the ways.
- Study Design: To gain the user perspective of the questions and the permutations and combinations required and to span it over two phases helped to attain knowledge how user interacts with the system or remembers his/her smartphone usage history.
- Assumption: The consideration of worst-case scenario. Here they considered that for the this fall back authentication the adversary has prior knowledge of the user. But still, the authentication scheme is able to distinguish between the legitimate and false users.

Major Critiques:

- The use of dynamic security questions for fallback authentication is novel. As questions asked during enrollment process of any fallback authentication, user tends to pick the easier questions. Thus, with the use of dynamic security questions the user is tested on the most recent memory.
- For proof of concepts the authors developed a prototype of two applications one for logging and other for questioning. The logging application logged the user devices information in background. User’s incoming/outgoing text and call were logged, along with application usage and music played. Questioning application generated questions based on the logged data.
- An ample amount of questions was asked in pre study, on an average 20 questions was asked to user and adversary. Users achieved 74% correct answers, but the adversaries achieved an accuracy of 51.3% in pre study. Furthermore, the authors are emphasizing on the usage of application usage and pattern.
- The use of timespan and to determine till which past to look for dynamic security questions is something intriguing and the authors were able to determine the best time span by asking the participants in the study and comparing their results.

- Authors in their work could have discussed some scenario where the adversary can determine the app usage based on the user behavior in common. For an example, if not the most popular social networking the applications, then the most commonly used application for any user can have high chances of using calendar, clock. These are now a basic application on any smartphone, but many users use them a lot to plan their day to week. Now, if the question application skips this as well there is high chance that there will be many false positives. As a user to remember which application he/she used yesterday or last week might be very hard to determine even for the users.
- Another possibility the attacker is do, is hard reset the device. Then none of the authentication scheme will prevail. There can be system lock to not to reset the device until and unless a valid authentication can be done. May be this might be out of scope. But I would perform an attack on this scheme as this using log and the log will be saved in some memory and hard reset using buttons can clear the memory. (Maybe out of context. But I would have locked the keys).

Minor Points:

- By not considering popular applications, the adversary is being challenged even more thus, making the scheme even more practical.

Conclusion:

- Authors have brought in the aspects of security questions which are currently deployed in emails and banking systems, to user fallback authentication. But these being dynamic in nature helps to create a scheme which user centric.
- Though, there are some drawbacks like a close adversary can take control of the device with the use of fallback authentication. But, with further analysis in the aspects of on the user behavior and combining these questions can lead to a better strong solution.

Gametrics: Towards Attack-resilient Behavioral Authentication with Simple Cognitive Games

Technical Summary:

Authors in [2] here developed a scheme called Gametrics which is based on cognitive games which is based on simple challenge, where the user needs to match objects with the targets by dragging and dropping them respectively. One of the motivations was to introduce enough randomization and at the same time keeping the scheme user friendly and short. The authors collected data from 118 participants to evaluate the authentication scheme. Based on the data collected on the interaction with the game based in mouse and cognitive ability the user various features were extracted. And passed through Random Forest Classifier, they achieved identification accuracy with a false negative rate 0.02%.

Contribution:

- The scheme is lightweight as it extracts 64 features from each game and capturing unique user interaction. The scheme was tested against zero effort attacks and active attacks like mimicking and shoulder surfing attack.
- The design of the game based on cognitive ability and making it user friendly. As user ease was considered while performing any authentication scheme. Additionally, the effort taken to get total 118 participants to test the scheme. Data collection was done across diverse age group and educational background. Thus, the challenges and the usability were tested across. Additionally, the authors had a 10276 challenges data. I feel data collection is very important when implementing any machine learning algorithm.

- Feature extraction is based on the gameplay time, time between the user pressing the start button to first mouse click to first drag/sweep of the mouse. Time between each drop and the drags of the mouse. The speed when the user is trying to find a target with object is being dragged. The silence between the drags and the move. And lastly the angle in mouse movement trajectory. In total 64 features are extracted based on these events and movements which, and also the combine effects are also studied.

Major Critiques:

- The game description, on how the picture frame was considered 500 X 300 pixels. And the details on how the object will be moving in the direction along with its average speed and the placement of targets. This detailed description really helped in visualizing the game.
- Cognitive approaches differed for users, for an example some users tried to comprehend the moving objects and their targets, few tried to start the challenge by completing the topmost target and its respective object. While others tried to pick the nearest object to mouse pointer. These approaches did show the cognitive way each user play.
- The authors did show, the reliability of the scheme by performing a shoulder surfing attack and including an attacker where he studied the user's movement through video recording. It did show that a single instance of the challenges had a false positive rate of 0.31 but the merged had 0.03. But in the realistic setting I feel the merged will be used.
- The bot attack was also considered where the bot acquires the template on how a user interacts and solves the challenge. But the bot can only mimic those it has acquired knowledge and the authors did try to randomize the challenges in their game design. Thus, making it difficult for the bot.
- Authors did try to tap on the exploitation of user cognition. But the scope is limited to computers or big screen devices. Cause using the same analogy on smartphone will be difficult as many people might have the same gameplay features as the touch dynamics will differ a lot on the small screen.
- I do believe this scheme can be used instead of the CAPTCHA scheme to determine a bot or human. But using it fall back authentication I will have my reservations as discussed in limitation, behavioral changes happened throughout life and its gradual even for us. Not just sudden changes and this might affect the authentication process as the template has some information which we were few months or years back.

Minor Points:

- The authors designed the game based on brands, animals and simple jobs. Which every user can understand and across all ages. Thus, the scheme got a good usable score.

Conclusion:

- The authors do provide an alternative scheme of authentication based on simple cognitive games. Thus, leading to ease in use of the system. Furthermore, the proof of concept was done across 118 users.
- The authors are able to achieve a 0.02 False Positive Rate for identification in merged challenges setting and thus giving us numerous applications where this behavioral biometric can be used. Thus, opening doors for future work on small screens and considering other parameters that can be used in cognitive authentication. One of the other parameters I might consider will be eye gaze and which corner of the picture or a target or the object does the user first try to memorize or capture. As this can also be a unique feature.

Behavioral Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality

Technical Summary:

The authors [3] provided a new way of authenticating user in VR systems. This scheme was based on s concept of continuous authentication by recording various body movements which the authors claim can be unique for each user. To make paper more understandable authors did define how the body movements are unique and how they can be recorded using VR devices and what kind of features can be extracted based on these movements. They achieved an accuracy of 63% for small group of 22 users. Though the accuracy is small the use of body combined body movements in VR for continuous authentication can be very helpful.

Contributions:

- To show explicitly on how each body movements theories effect the biometric in human. By showing the in-depth study of the coordinated body movements the authors showed how these movements can be captured in a VR system.
- The use of motor control where the user/human tries to stabilize or maintain equilibrium in various activities can be unique. Proception where the user tries to sense its relative position, muscle and joints movements with each other. They even exploited view relation, which is based on eye gaze. World Reference and Target here in the VR system the target can be at certain position and how the user tries to reach it can be different strategy for each of them.
- Based on the body theories, they designed activities which can combine the above four in the VR ecosystem. Author considered the following activities pointing to a target, grabbing activity (In VR is reaching the target and clicking and releasing), Walking as the user navigates in virtual space by physically walking and typing in VR was recorded with the help of handheld raypoint controller.
- Feature selection was optimized and used. They did this by using wrapper-based feature selection using greedy based algorithm.

Major Critiques:

- By studying the body mechanisms and bottling down the activities, authors were able to determine the features need to be extracted from and which can correlate body activities (Requiring more than one movement of the muscles and joints) with the VR ecosystems extracting features.
- They considered the dominant and non-dominant hands and its affects, head movements, eye gaze. For each of the VR equipment's they logged position, rotation, velocity and angular movement. As well as current gaze points and collision points were recorded for the VR headset and handheld controller.
- Based on the data collected the features they extracted were based on Individual sensors, combining two motion types into one feature set, distance based on Euclidean, distance between target and the device. Visual angle for the target and all of the visual angle with respective to the user. And combining all of the features in one category or taking one feature of one category.
- Defining the use of this authentication scheme on smaller group size and the reason and importance of this. Cause VR ecosystem will initially enter the home environment and the implicit authentication help in parental control.
- The authors considered walking with head movements. But there are many works that do show that an arm swing of a user's does show high accuracy while identifying the user. The raypoint controller must be having a motion sensor giving data on acceleration, angle and gyro data. Thus, achieving a low identification accuracy is something I would look into it more.

Minor Points:

- Many of the biometric activities work do not explain the body movements in such depth. Being a reader, I was fascinated way it was presented including the figures.

Conclusion:

- Though the authors achieved a lower accuracy across all the activities. But the intuition behind extracting the data and including the actual body movements theory is something out of the box.
- Furthermore, I believe the VR headset will be first penetrating the home setting first and the authors were able to achieve a good accuracy in small user setting. Thus, continuous authentication in this setting can be really helpful.
- Furthermore, they were able to determine and prove that pointing activities are more accurate in VR ecosystems than grabbing. Thus, a new activity can be considered in the future work with pointing activity in mind.

Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication

Technical Summary:

Authors [4] discussed a continuous authentication approach on the touchscreen of mobile devices. This authentication scheme can act as an additional layer of security once the user authenticates himself/herself with a traditional scheme. The authors proposed 30 behavioral features that can be extracted while the user is interacting with the touchscreen. They developed an android application for collecting the data which was based on fingertip action which were sliding horizontally and vertically. The authors used two classifiers to test their data kNN and SVM and achieved an accuracy of cent percent for intrasession, 2-3% for intersession and below 4% for intraweek authentication. They performed various authentic scenarios for users as mentioned earlier. This paper does give a pathway on how to go ahead with continuous authentication in smartphone using touchscreen.

Contribution:

- The guidelines the authors decided to go through while conducting the study, did help to get a true practical scenario of the users while operating the smartphones. The user was given the freedom on however they want to operate the smartphone while reading, but it was limited to the use so that user will need to pick up the device giving higher chance in change orientation of the phone.
- A stroke trajectory was an encoded sequence which incorporated various sensors values all together under one tuple. Thus, making the label for the users much easier.
- Removing the dependence stoke location on the screen area where user tends to operate most of the smartphone helped the user to have more freedom in operating the device. Considering the fast scrolling mechanism in the touch dynamics, helped them to attain a new feature called median velocity of the five points.

Major Critiques:

- The computation mutual information among the features and its impact to see how user behavior differs with respective to each feature. This helped them which feature they can use in classification cause one with most information cab lead to identifying the user easily.
- The use of two classifiers kNN and SVM and the evaluation results for them showed an equal error rate of 2% to 3% at 11 to 12 stokes. This evaluation gave the authors the time duration till which an intruder can be detected in the scheme.

- The evaluation of interweek authentication where the user is training the classifier a week and then it he/she has picked the phone to get authenticated. Intersession authentication where the user needs to be authenticated on the same day over multiple session and lastly short-term authentication this when the classifiers start to learn the user after completing the primary authentication and then keep on testing the legitimacy of the user. They achieved an accuracy ranging from 0-4%.
- Though this paper shows how touch dynamics can be considered, but a brief study on shoulder surfing attack or mimicry attack can tell us in depth how well this scheme can withstand. Additionally, the device with a same make and model, the users tends to use the similar screen areas on the phone, if the users share a similar body as well.

Minor Points:

- The Fig 2 could have been at the bottom of the page instead just below Table 1. This might confuse many readers.

Conclusion:

- The authors did provide a groundwork on how touch dynamics can be used in multi authentication schemes.
- But for future work, I would consider touch dynamics of the users for every new application installed. Cause every user will interact with the application screen in particular way. Thus, giving us understanding if the application is installed by owner or not. Thus, giving us better parental control as well. It's just a thought.

Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It but You Can Not Do It

Technical Summary:

Authors [5] here proposed an authentication scheme which was gesture based called GEAT on the touchscreen of the smartphones. GEAT acquires 15 to 25 samples of the user's gestures on the screen and extracts and selects behavioral features that later passed to a Support Vector Distribution Estimation classifier to obtain the legitimacy of the user. One of the motivations for proposing this solution was GEAT is not suspectable to smudge attacks which are seen on fingerprint and pattern-based authentication techniques. They selected 10 gestures for GEAT which the user had to perform during the study. They showed GEAT can be lightweight as well by taking only 3 gestures and 25 samples it achieved an equal error rate of 0.5%. Additionally, the authors did a real-world evaluation by performing zero knowledge-based attack and shoulder surfing attacks to test authentication scheme.

Contributions:

- Selection of 10 gestures out of 39 gestures. Selection of effective features based on these gestures that capture the behavioral information on the touch screen.
- Segmentation of strokes into sub strokes. This was really important for this scheme as each stroke had different time, thus segmenting it into sub strokes and selecting the ones which have the same time duration helped lot in the authentication scheme.
- Data collection of 15009 training samples from 50 users for proof of concept for GEAT. With such huge data set does help the evaluation of the scheme.
- Evaluating the scheme against shoulder surfing attack by allowing attacker to study the gestures of the 10 users by a video and performing the attack does provide a solid proof. Additionally, a zero-effort attack was also done on the scheme. Thus, giving us a real-world application detail.

Major Critiques:

- Authors normalized the time series data to bring all the values in the range of 0 to 1. This was done to find the similarities between two signals. Additionally, before normalizing the authors made sure the two signals have the same number of elements by resampling one of the signals.
- Features were considered based on velocity and acceleration magnitude, stroke time, inter stroke time, stroke displacement, and velocity direction.
- As the data was of time series which was logged from a capacitive touch screen which introduce noise in the data. They used a moving average filter to get a less noisy data.
- The discussion of the tradeoff of usability vs security with the classifier. And justifying the use of highest value for true positive rate. They did this by synthetic imposter on the GEAT classifier which was not included in the training phase.
- Not a machine learning expert but isn't more data on training sample for any particular user will give more thorough classification. Though they have justified the increase in training sample size increases the equal error rate. But I feel that the data analysis needs more work cause, this means the features extracted are not that distinct.

Minor Points:

- This work has shown gesture-based authentication can be used. But a more evaluation on attacks especially the smudge attacks would be more helpful. As, pattern unlock is also a type of a gesture.

Conclusion:

- This paper did bring a new way of unlocking a smartphone using gestures and authors did a very good job in proving the concept.
- For future work, I would consider the authors to use pressure on the screen, relative orientation of the device with respect to ground (Phone kept on table will always have different orientation as one kept in hand).
- As user keeps accustomed to certain gesture the speed and acceleration of the performing the gesture will also increase. Then in this case does the classifier will classify a legitimate user as an imposter cause the features extracted are based on time and accelerations.

Bibliography

[1] A. Hang, A. De Luca and H. Hussmann, "I Know What You Did Last Week! Do You?: Dynamic Security Questions for Fallback Authentication on Smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, South Korea, 2015.

[2] M. Mohmamed and N. Saxena, "Gametrics: Towards Attack-resilient Behavioral Authentication with Simple Cognitive Games," in *Proceedings of the 32Nd Annual Conference on Computer Security Applications*, Los Angeles, California, USA, 2016.

[3] K. Pfeuffer, M. J. Geiger, S. Prange, L. Mecke, D. Buschek and F. Alt, "Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland Uk, 2019.

[4] M. Frank, R. Biedert, E. Ma, I. Martinovid and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," *IEEE Transactions on Information Forensics and Security,* vol. 8, pp. 136-148, January 2013.

[5] M. Shahzad, A. X. Liu and A. Samuel, "Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You Can See It but You Can Not Do It," in *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, Miami, Florida, USA, 2013.