Black Team:
Joseph Cox
Tom Nguyen
Fariha Moomtaheen

Project Description

Data Acquisition:

We will be using the data provided to us and maybe collect or own data to create a User Device Interaction Verification Survey (UDIVS). Due to the nature of our project, it does not require data enhancement or noise reduction. But, we will use data analysis techniques to ask specific questions about the user's recent activities, which means that data set would have to adjust over time. Based on their answers it will create a score that can either grant or deny access to a system.

Feature Extraction:

We will be using features such as application, text messages, networking activity, calling, and maybe location. Based on the frequencies of the data we collect, we will ask a series of questions that will validate the user by asking questions about frequency, time, and sequence of the events/categorical data that occurred while the device was being used. We plan on using score-level fusion, not feature level fusion. But the questions we ask will be based on the data we collect from the features. The (UDIVS) will generate questions based on selected features. Ideally, a combination of activities that are frequent and infrequent will be used. The goal is to use one hot encoding to extract features to generate a combination of questions based on activities within a timeframe so that it is too difficult for an imposter to spoof the system, but at the same time easy for the genuine user to get a high enough score to be validated by the survey. This also means adjustments will have to be made to the data set. How far back in the users history should the questions be asked? This is a window of time that needs to be considered as we develop and test the system. If the data is too recent asking effective questions may be difficult and the False Acceptance Rates may increase, if it is too far in the past the user may not be able to remember what activities they did, thus increasing the False Reject Rates. A sliding window approach is appropriate to consistently update the data to ask questions relevant to recent user activity. What the window size should be is unknown and something that will have to be tested.

Matching:

According to Lecture 6 slide 4, there are no standard methods to extract or match features for user-device interaction based biometrics. Our plan is to give some points to each option of a multiple choice question and calculate the scores from them. We will not use machine learning for matching as we are not teaching the system to gradually learn to customize its behavior according to the user. Rather, the system just observes the user and asks them questions based on their activities. There is no need for any distance measures either as this is purely a question and answer based system. The UDIVS will use score-level fusion for generating scores for a user. If the final score satisfies a certain threshold the user can be verified as genuine. The final score will be generated from the scores credited for each question. If a question has multiple correct answers, a person will get some points for identifying some of them and gain negative points for a wrong choice.

Decision:

Our UDIVS system uses a single biometric modality that computes a single matching score for the decision process. Computing the actual score requires a separate decision process determined by the features used. For each verification process, a user is prompted with a series of questions. Each question produces a matching score by using an ‘AND’ or ‘OR’ operation that is then fused. For instance if there are two correct answers the user may or may not get points for one correct answer. For a question that has two answers and zero points is awarded for only one correct answer than that would be an ‘AND’ operation, and if points are being awarded for one correct answer that would be an ‘OR’ operation. In this context, this would be similar to a decision-level fusion. The subscores are consolidated into a final score, by a score fusion technique, to compare with the threshold. Essentially, the subscores from individual questions are derived from fusion, but the final decision is singular purely because our system is uni-biometric.

Why did you choose this project, how was it motivated by Part 1, and what do you expect to gain from carrying it out?

Given that most of the research articles that our group read is in gait, keystroke, and touch gesture from part one of the project, we became

intrigued with user-device interaction. One of the biggest concerns in biometric verification, as defined in one of the articles, is generating a high performance, reliable, and low cost verification system, which we hope to satisfy with our UDIVS. Reading about the proposed 3D graphical password verification[1], one of our chosen articles, inspired us to cement the groundwork for a new validation system. We also must configure an optimum threshold value that ensures an accurate verification process. In general, we are genuinely interested to study user-interaction and potentially expand its versatility to one-off verification. We will attempt to implement an android demo to introduce us to new skills and to further test if such a system is plausible, convenient, and user-friendly enough to be adopted by smartphone users.

How might this project address a current challenge?

Knowledge-based recognition is still widely used for typical logins, but it's ultimately plagued by shoulder surfing, smudge attacks, the need for long-term memory, keylogging virus attacks, and other spoof attacks. Our UDIVS provides a dynamic verification method that relies on querying the user based on their device interaction. In other words, we ask users a series of questions about their recent activity. If this mode of verification proves to be feasible, our system could mitigate the issues with memorizing pins and passwords. This would abate spoofing attacks since the answer and question changes with each verification prompt. It could also reduce the security compromises with reusing a password for multiple logins. Another issue that it solves is if a user is able to, for some reason, be verified by the system, there is a good chance that they will not be able to enter it a second or third time. Unlike passwords, fingerprints, and face detection, if a wolf is able to spoof the system once there is a good chance that it can happen again. With this system, since the questions change a wolf may not be allowed re-entry, thus limiting the amount of damage a wolf can do overtime.

Citations:

[1] Z. Yu, I. Olade, H. N. Liang, C. Fleming, “Usable authentication mechanisms for mobile devices: An exploration of 3D graphical passwords,” In Proc. Int. Conf. Platform Technology and Service (PlatCon), pages 1–3, 2016.