Title: Surveying the Development of Biometric User Authentication on Mobile Phones

Team color : Black

* Face features can be classified into 3 folders: Traditional, Three dimensional, and skin texture.
* Behavior profiling related features: General applications (app name, date, time of usage, and cell ID). Voice call (date, time, number of calling, duration and ell ID). Text message (data, time, number of texting and cell ID).
* Meng considered multi-touch as a key feature. On the Nexus One phone, Meng achieved an FAR of 2.5% and FRR of 3.34% with a combined classifier of PSO-RBFN.
* Behavioral biometric authentication can overcome the issue of one-off Authentication on mobile phones.
* Voice, signature, gait, behavior profiling, keystroke, and touch are all viable for continuous authentication with touch growing rapidly popular.
* Touch dynamics is cheap. Requires no special or additional hardware. Continuous and transparent user authentication method. However, it has lower accuracy and deals with user inconsistencies.
* Physiological authentication has higher accuracy but usually one-off and needs additional hardware.
* TouchLogger (infer keys typed) and TapLogger (log keystrokes)
* Smudge attacks. Residual oils on screen. Used to track touch inputs.
* Anomaly detection can be used after one-off authentication.
* Draffin, proposed a passive authentication method by modeling micro-behavior of users’ interaction with soft keyboard. From specific location touched, drift of finger, force of touch, area of press. Identified imposter user within 5 key presses 67.7% of time.
* Key things to design authentication system: better than knowledge based methods, transparent method, continuous and periodic after one-off, works across many mobile OS, easy on workload, appealing for users (high acceptance).
* 3 security measures: Alert Level, Tolerance number, Actions & Responses. When all trials of the tolerance number have failed, the alert level increases which determines the next action & response.
* Cloud-based framework reduces overhead and supports more complex computations.

Title: Biometric recognition by gait: A survey of modalities and feature

Team color : Black

* Gait began with image processing, but new methods were utilized such as derfoot pressures and accelerometer.
* USF supplied a significant portion of data to the HumanID dataset challenge. It is the most commonly used dataset in gait recognition literature.
* Various modalities should capture biomechanical pressures, its body part masses, or the time-varying generated forces applied during gait.
* Common preprocessing step is to extract a binary silhouette. From this, we can obtain the width and build of the silhouette.
* Pressure mats were able to normalize the orientation and position of footprints and matched with direct templates. Mat can compute spatial features and between-footstep features (e.g., stride length, toe-out angle), and indicate barefoot travel.
* Rodriguez 2011;2013 extract contour features in the pressure, captured negative and positive changes among the sensors at each time stop.
* Find acceleration by F=ma. comparing gait cycle accelerations achieved the lowest EER (<10%).
* Acoustic Gait features: may be more accurate than pressure data. Audio records a sense of intensity as well as measure the time between footsteps. The cadence of the sound can determine cycle.
* Gafurov et at. (2007) evaluated spoofing by comparing average gait cycles approach achieved a 73.2%. Performance CR with 100 subjects.
* Subjects mimicking other gaits caused CR drop to 50 from 90 total.
* 6 challenges in biometric gait recog: Distinctiveness of cue. Consistency with time, emotion, and illness. Effects of covariate and spoofing. Fusion of gait with other sensors and biometrics. Prediction. Create dataset. Explore role of deep learning in gait.
* Cross-modality prediction of gait features: Predicting gait feature sets pertaining to one modality based on another modality. Side q: Can a gait be accurately modeled based on a few features?
* Consistency of gait: GRF curves report the change in overall vertical force over the footstep, and COP curves provides the underfoot trajectory.

Title: A survey on touch dynamics authentication in mobile devices

Team color: Black

* Important factor in influencing people is usability. There are 2 primary usability issues: slow performance and inconvenience, and social awkwardness.
* Touch dynamics is a behavioral biometrics modality, which can be used with passcode authentication as a multi-step authentication. process. This is done by using sensors embedded in the screen.
* Touch dynamics have multiple features: Distinctiveness, Familiarity, Enhanced Security, Cost Effectiveness, Continuous Monitoring, Revocability, Non-dependency, and Transparency.
* Touch in conjunction to pass codes adds extra security and this is also beneficial because pass codes are still the most widely used security method.
* Some challenging issues and potential research topics are: Minimizing Computation and Communication costs, Minimizing energy consumption, Maximizing accuracy, Adaptation.
* There is an energy tradeoff to have a touch process that is continuously checking and authenticating could consume power so sampling of the data is limited.
* Verification-in-Dynamic mode is continuous authentication. This form checks the user in samples/intervals periodically.
* In an experiment you must set the control, which means predefined restrictions. Two types: 1) Supervision, 2) unmonitored without restrictions. Just enough control to reduce variation and noise.
* For input size generally speaking the larger the input size the more accurate the data is and its ability to determine all the nuances of the user or imposter, the larger the sample the better the subject is represented in the data.
* Sen et al. proved touch dynamics combined with digit-based passcode to be able to fend off wolf attacks.
* Probabilistic modeling is the most used & statistical measure is the least used technique adopted by researchers. Reason being to predict touch gesture actions.
* Sen et al 2014 used touch dynamics to enhance PIN. FRR was at 14%. Two imposters were instructed to attack the PIN by mimicking the legitimate user’s keystroke features with an FAR of 16%.

Title: Surveying Biometric Authentication for Mobile Device Security

Team color: Black

* Behavioral biometrics have been referred as “transparent, continuous, implicit, active, passive, non-intrusive, non-observable, adaptive, unobtrusive, and progressive.”
* Knowledge-based suffer from memory load, shoulder surfing, smudge attacks, password reuse, and user inconvenience, and provides same level of security for all authentications.
* Gesture Doodling (interesting tactic) reduced log-in time by 22%.
* Motion based sensors (i.e accelerometer, gyroscopes) help reduce from rotation, angles, and orientation. Helps in normalization.
* Periocular feature levels: Level 1: general/holistic, eyefolds, eyelids, moles, wrinkles etc; Level 2: detailed, texture and hair follicles.
* Iris possibly most accurate bio-trait. From one study, EER of 0.14%.
* Some iris scanners use infrared sensor, which could potentially damage the eye.
* An efficient mobile device authentication should improve security beyond point-of-entry, reduce auth. attempts via transparency, provide continuous auth., and works cross-platform/cross-hardware.
* Single knowledge-based auth. allows intruder to complete 1k tasks after 1 successful attempt. Multimodal allows 1 task for 6k attempts.
* Keystroke and touch dynamics can be enhanced using other sensors.
* There is evidence of relationship between thumb length and swipe gestures in completion time, speed, and acceleration. Correlation b/t biological anatomy and touch gestures.
* Behavior profiling features: categorized features, frequency features, and sequential features.
* Direct attack: presenting fake/false traits.
* Indirect attack: intercepting between channels/interfaces.
* Common properties with protected templates: noninvertible, revocable, unlinkable, diverse, and system performance.
* Salting, noninvertible transform, key-binding biometric cryptosystem, and key-generating biometric cryptosystem are 4 template protection schemes.
* B/c behavior is not permanent, there needs to be software to maintain updated biometric templates.
* Gait data is only useful when the user is in motion. When idle or sitting shift to another mode of authentication.

**Paper One:**

Who are the researchers?

D. Damopoulos, G. Kambourakis, and S. Gritzalis, “From keyloggers to touchloggers: Take the rough with the smooth,” Comput. Security, vol. 32, pp. 102–114, Feb. 2013.

What did they do?

Investigate the potentiality of touchlogging on smartphones for behavioral profiling. This included keystrokes and touch gesture analysis.

Where did they do it?

The actual login is performed on a variety of user owned jailbroken iPhone with iOS 4.0. The data analysis is performed on a “2.53 GHz Intel Core 2 Duo T7200 CPU and 8 GB of RAM” running OS X Mountain Lion

How did they do it?

They created an application called iTL, a touchlogger based in Objective-C with two major class components, a gesture logger and a keylogger named iGL and iKL, respectively. The experiment called for 18 iphone users from ages 22 to 36. Each participant used their iphones normally for 24hrs a day. Data of gesture and keyboard use were logged. After data collection was completed, the data file was transmitted via Wi-Fi to a remote server for analyzation. For classification, a file was created for each user that contained the legitimate user’s data and all other users’ data representing imposters. Each record contained 4 information; the type of event, the location in x, y coordinates, the timestamp, and whether the user was classified as an intruder or legit. Then using 4 different machine learning algorithms, then found the FAR, FRR, and the EER for each method.

Why did they do it?

Keyloggers were originally popular due to physical keyboards used on cell phones. This literature reveals how data can be collected on a touchscreen device, similarly to how a keylogger collects data. They’ve also expanded beyond logging soft keyboard presses with touch gesture recording.

What are the remaining problems/future work?

The researchers will continue gathering more data and analyze them more thoroughly. They hope to enrich and improve the current dataset.

**Paper Two:**

Who are the researchers?

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.

What did they do?

The researchers created a program that allow users to create a 3D password using hand motion with their mobile devices.

Where did they do it?

Used Unity3D package and scripting in C#. There didn’t seem to be a specific location, but it was assumed to take place in a controlled environment for 3D spatial movement. We can also assume a higher spec computer was used to develop and run the technology.

How did they do it?

To interface between the user and mobile devices, a Leap was used to capture hand movement in a virtual 3D space that can be displayed on the mobile device. The actual software utilizes a cubic matrix consisting of edges and nodes. Movements in the 3D environment is traced as a sequence of edges and nodes. As for the actual user interface, there are 8 cubes uniformly distributed. The user interacts by drawing lines from these cubes in a virtual 3D space with the Leap device. The pattern sequence is processed by an algorithm which creates a new password based on the pattern for login verification.

Why did they do it?

The research demonstrates the feasibility of 3D graphical passwords in a 3D environment. They also provided a new mode of authentication that can be implemented on mobile devices.

What are the remaining problems/future work?

They need to examine the usability of this technology on mobile devices. Only cubes were used, so there are plenty of shapes and elements to work with to increase security measures. They also hope to eliminate the need for an external device so that users can authenticate using only their phone

and hand. A survey is necessary to gather public opinion on the adoption of 3D graphical passwords on their mobile devices.

**Paper Three:**

Who are the researchers?

G. Ho, “TapDynamics: Strengthening User Authentication on Mobile Phones with Keystroke Dynamics.” In Stanford University, 2013.

What did they do?

The author established the security and usability for one of the behavioral biometric methods- keystroke dynamics. The paper explores more features than previously implemented in the case of mobile devices and is the first one to apply them to short 4-digit pin codes. The features are put into 4 kinds of classifiers to be analyzed.

Where did they do it?

The researchers developed an Android app to collect data from user’s input. But as the download or installation of any software is prohibited by crowd sourcing services like Mechanical Turk, the researchers had to submit the request to the Institutional Review Board of the Stanford University. Their procedure keeps users anonymous and doesn’t collect other personal data which got it clearance as a non-human subject research. Finally they manually collected data and gathered enough to continue work.

How did they do it?

They collected fifty five unique user’s input and built an accelerometer profile based on the features collected per training example. The choice of classifiers covered the two most used classifiers- Manhattan Distance Classifier and Random Forest Classifier, then the Gaussian Discriminant Analysis because of the nature of the features and finally the SVM because it is very rarely regarded in literature. Then they generated the FAR and FRRs of all four classifiers to analyze the security and usability. Finally they adjusted the training and test examples to get over the issues detected, like overfitting and found satisfactory results especially for the SVM classifier.

Why did they do it?

The training example contained 5 features and accelerometer readings. The authors theorized that combining them to build an accelerometer profile would be more practical in order to uniquely identify correct user.

What are the remaining problems/future work?

The paper showed promise that increasing positive training example will yield better scenario and increase usability of classifiers. So more techniques to create synthetic positive examples can be explored in future works. Also, to be able to extract interesting features from accelerometer readings and do them intelligently can be a vast field of work for this research. The research showed an uncommon result for the GDA model and future work can focus to explore and analyze that problem.

**Paper Four:**

Who are the researchers?

N. Zheng, K. Bai, H. Huang, H. Wang, “You Are How You Touch: User Verification on Smartphones via Tapping Behaviors“ In IEEE Int. Conf. on Network Protocol, Dec. 2014.

What did they do?

Utilizing smartphones, the researchers added tapping feature detection to passwords/codes to enhance security. They collected data on 8 digit pins and 4 digit pins that were preset to ensure different parts of the screen on the smartphone are utilized. 80 different subjects were required to enter a pin in 25 times each without error. Over 11,000 error free samples were collected in the data collection process. They examined the feasibility and performance of a system that used tapping behavior frequency in conjunction with passcode entry by a single and double classifier machine learning algorithm. They also analyzed the system overhead for memory and run time complexity for passcodes.

Where did they do it?

The research was done at multiple places: College of William and Mary, Williamsburg, VA, USA, another is at the IBM T.J. Watson Research Center, Yorktown Heights, NY, USA and the University of Delaware, Newark, DE, USA. But the paper states that the data collection was done at the College of William and Mary “we invite graduate and undergraduate students in our institution to participate in this study”.

How did they do it?

They developed a single classifier and two classifier machine learning algorithm based on the data they collected. They computed four sets of data: acceleration, pressure, size, and time and looked at the uniqueness and pattern of each of these data sets. This data is then feed into a classifier that then produces a decision score based on comparing the raw data to the target template. The decision score is used by a decision maker that finalizes and determines whether the tapping action is from the target or imposter based on threshold values. They extracted and tested the data that they collected in different positions and environments to ensure the quality of their data and accuracy.

Why did they do it?

They did this because physiological methods of authentication are problematic when the environment changes. This causes accuracy errors and lowers the dependability of these methods. Utilizing touch tapping frequency in conjunction with passwords provides an extra layer of security as well as more reliability. Tapping data does not depend on things like lighting and camera angel like vision does. It does fingerprints also may depend on the surface being clean etc. Tapping also has a familiarity factor to many users as well. The paper calls it implicit authentication, and the researchers believe that it is both “cost effective” and “user transparent”

What are the remaining problems/future work?

Remaining problems are accuracy especially when data is collected from multiple positions. In their future work they will have a larger data set with positions, but another problem arises when this occurs. If more data is to be acquired to drop the EER, it will require more processing power and memory. So the memory overhead and processing power will increase, mobile devices are not desktops and they have limited memory and processing. Mimic attacks are a problem as well, their algorithm is crackable if the imposter can simulate a similar frequency to that of the target. Behavior changes also can pose a problem and increase the false reject rates, what if a user breaks their thumb? Password changes are also an issue and could reset the whole machine learning algorithm and require new training sessions.