Spoof-resistant Authentication Through Phone and Wearables

PIs: Vir Phoha (Lead, Syracuse University); Nitesh Saxena (UAB); Abdul Serwadda (Texas Tech)

The objective of this project is to develop a secure and easy-to-use mechanism of continuous user authentication for the current generation of smart phones

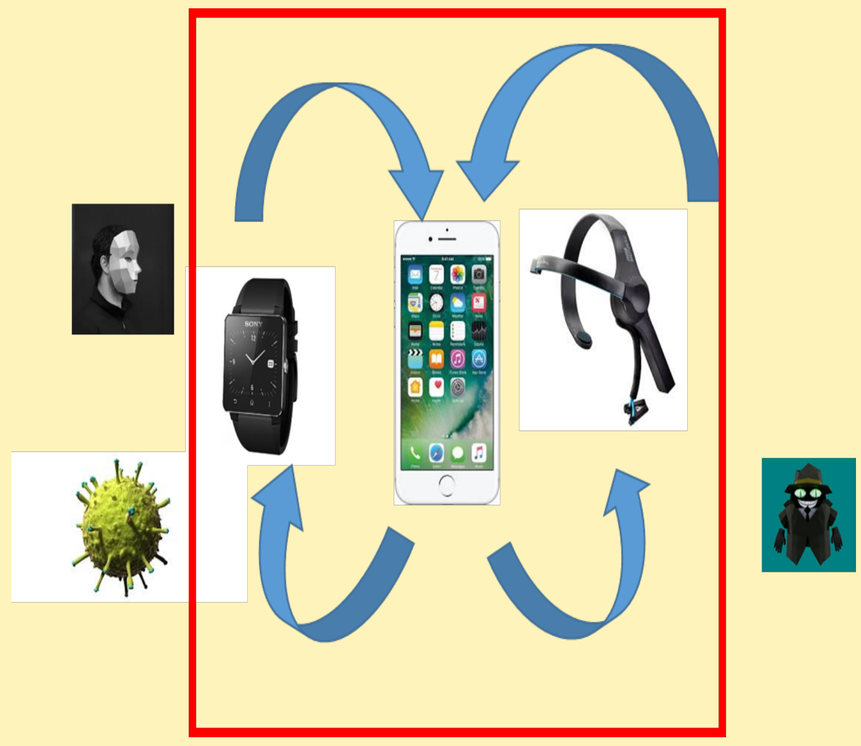
Continuous Authentication System based on Multi-Modal Wearable Devices:
Measure movement dynamics of different body parts (e.g., head, eye muscle, hand and wrist) and neuro-physiological characteristics (e.g., brain wave and eye gaze patterns)

Spoofing Attack Modeling and Analysis
Develop mechanisms to defend against active adversaries who may resort to robotic and sensor-spoofing attacks

System Usability Evaluations
Develop evaluation mechanisms focusing on not only authentication efficiency and accuracy but also user experience and user perceptions

Devices and Respective Features

- Movement Patterns using Inertial Sensors (on phone, watch and glasses)
- Brain activity Patterns from EEG Sensors (on BCI headset)
- Eye Movement Patterns (on glass)
- Touch Patterns (on phone)



Global view of our device interconnection setup

Approach

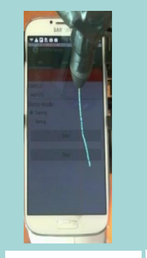
Template as, $T = \{TIP_1, TIP_2, \ldots, TIP_n\}$, where P_1 to P_n are the base activities such as walking, standing, etc.

Assuming availability of data from smart watch, BCI devices, etc. update each of the sub-profiles in T to include information from the other sensors.

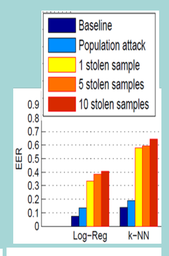
Fusing Devices and Sensors (including Preliminary Results) Classification Algorithms to be Studied
Fusion: Naïve Bayes; Weighted majority voting; Code alignments
Classifiers: Naïve Bayes, 2) Tree Augmented Naïve Bayes, 3) Logistic Regression, 4) k-Nearest Neighbor, 5) Scaled Manhattan, 6) Support Vector Machines, 7) Scaled Mahalanobis, 8) Neural Network, and 9) Random Forests.

Spoof Attack Modeling and Analysis

Illustrating how robot holds stylus and phone during attack



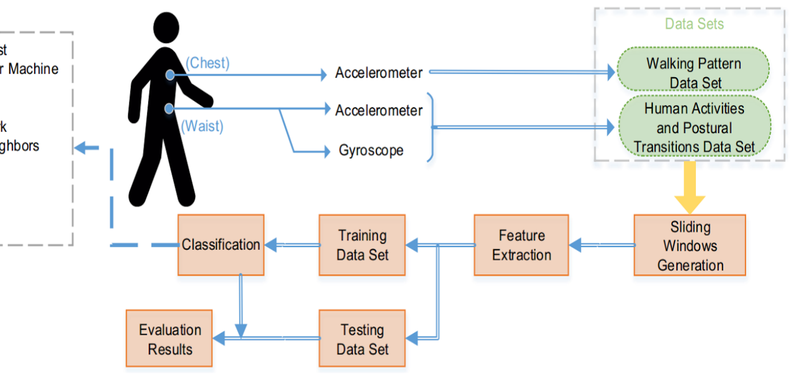
A touch stroke executed on the phone screen



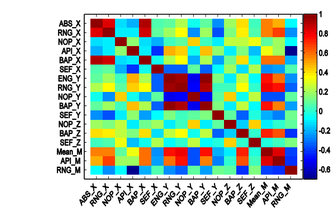
(c) Performance of different forms of the attack

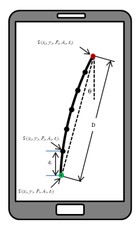
Spoofing the swipes

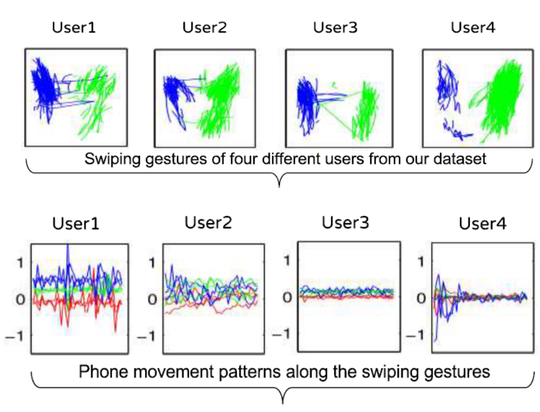
Spoofing the walk



Comparison of classifier performance through behavioral patterns obtained through phone







Fusion of different activity patterns

Publications

R. Kumar, V. V. Phoha, and R. Raina, "Continuous Authentication of Smartphone Users by Fusing Typing, Swiping and Phone Movement Patterns," in *IEEE BTAS*, Buffalo, New York, 2016

A. Serwadda, V. V. Phoha, Z. Wang, R. Kumar, and D. Shukla, "Toward Robotic Robbery on the Touch Screen," *ACM Transactions on Information System Secuity.,* vol. 18, pp. 1-25, 2016

C. Tang and V. V. Phoha, "An Empirical Evaluation of Activities and Classifiers for User Identification on Smartphones," in *IEEE BTAS*, Buffalo, New York, 2016.

Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena and N. Asokan , Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks. In the Network and Distributed System Security Symposium (NDSS), February 2016

Babins Shrestha, Manar Mohamed, Sandeep Tamrakar and Nitesh Saxena, Gametrics: Towards Attack-Resilient Behavioral Authentication with Simple Cognitive Games, In Annual Computer Security Applications Conference (ACSAC), December 2016

Babins Shrestha, Manar Mohamed, Sandeep Tamrakar and Nitesh Saxena ,Theft Resilient Mobile Payments: Transparently Authenticating NFC Users with Tapping Gesture Biometrics, In Annual Computer Security Applications Conference (ACSAC), December 2016

- **Activities:**
  - **Dynamic**
    - **Walking**
    - **Walking upstairs**
    - **Walking downstairs**
  - **Static**
    - **Sitting**
    - **Standing**
    - **Lying**

Transitions:
- **Sit-to-stand**
- **Stand-to-sit**
- **Sit-to-lie**
- **Lie-to-sit**
- **Lie-to-stand**
- **Stand-to-lie**

Type	Activity	RF	SVM	NB	J48	NN	kNN	Rpart	JRip	Bag	AB	Average
Dynamic	Walk	**97.6**	89.7	**92.4**	89.7	**97.8**	**100.0**	78.5	80.5	87.7	**97.8**	**91.2**
	Upstairs	**93.6**	79.6	82.9	82.7	**90.5**	**100.0**	71.4	71.2	80.9	**91.4**	84.4
	Downstairs	**94.6**	71.4	78.0	80.2	86.3	**100.0**	68.2	67.2	79.2	**95.6**	82.1
Static	Sit	68.3	22.2	12.9	69.2	62.9	**99.8**	33.7	48.1	44.3	46.4	50.8
	Stand	72.2	37.5	25.6	74.1	76.8	**100.0**	52.6	60.7	57.9	59.8	61.7
	Lie	86.6	46.9	34.7	84.1	80.6	**99.8**	58.8	72.4	66.5	84.5	71.5
Aggregated	Aggregate	86.3	30.6	10.1	80.0	40.2	**100.0**	14.8	62.8	16.1	18.5	45.9
	Aggregate*	83.4	30.0	10.0	77.1	41.7	**100.0**	14.8	58.0	16.7	18.7	45.0
	Aggregate**	80.9	29.2	10.2	74.8	35.3	**99.2**	14.6	57.0	16.4	15.7	43.3

Contact: Vir V Phoha; Email: phoha@acm.org

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9 –January 11, 2017
Arlington, VA