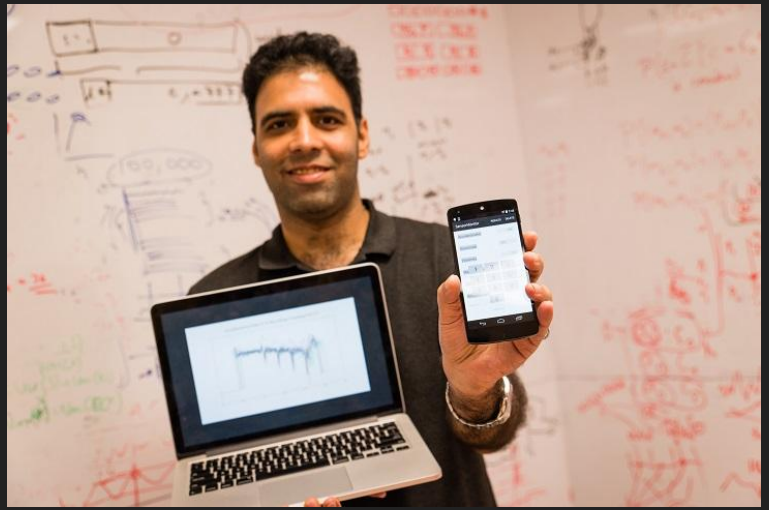
There goes your PIN

Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting

Hackers could guess your PIN using its sensor data

- Researchers at NTU found a vulnerability inside 6 basic sensors on smartphones.
- Accelerometer
- Gyroscope
- Magnetometer
- Proximity Meter
- Barometer
- Ambient light sensor



Improvements compared to previous work

- Not the first time hackers are trying to take advantage of those sensors…
- From 74% to 99.5% success rate of 50 chosen password in a single try
- (New) Random password, 83.7% success rate in 20 tries.
- (New) Cross User Scenario
  - Recovering PIN from a new user.
  - Reducing user interaction to Min.

How is it done?
Why has it improved so much?

- Powerful Machine Learning Algorithms
  - Multi-layer perceptron (MLP)
  - A limited memory Broyden Fletcher Goldfarb Shanno (L-BFGS)

- Zero-permission Sensors
  - Exploited by an attacker, without the knowledge of the user
  - Relatively easy to gain a lot of data
- Different Approaches used

Let’s go into details

Assume we have a 4 digit PIN right now…

1. The first approach uses the complete data stream and associates it to the combination of keys during the training phrase. 10000 combinations.

2. The second approach identifies single digit individually by first splitting the data into parts corresponding to the individual presses. 10 digits.
    - More flexible, no need to change amount of data when digits increase
    - Difficulty in right timing

Let’s go into details

- Body Position, Holding type, Speed, Left or Right Hand…

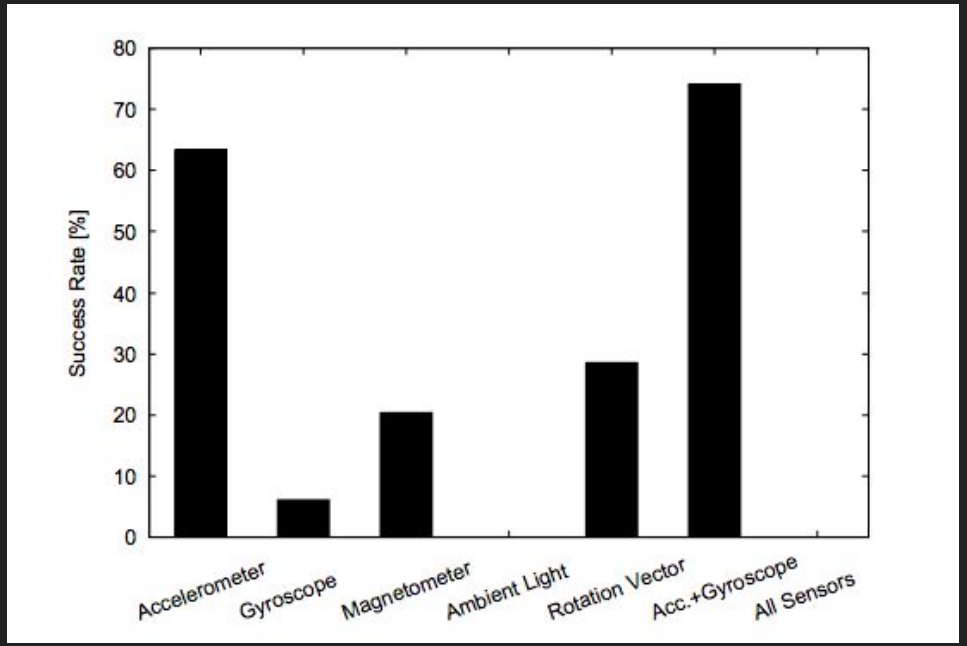
  These physical factors affect the weights of each sensor

- Created a two dimensional array to do classification algorithm
  - MLP
  - L-BFGS

Result

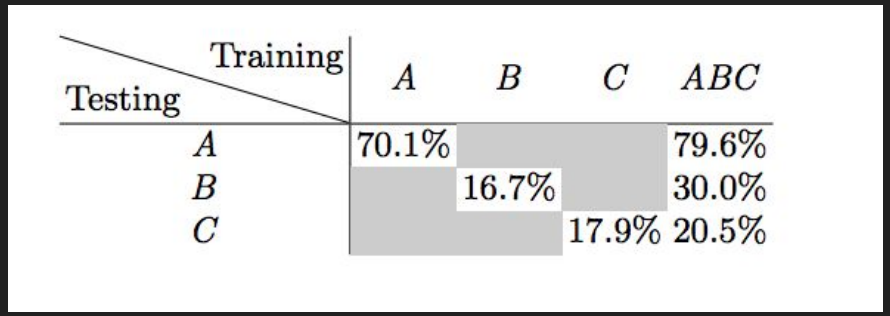
- Individual Sensor Success
  - Accelerometer (63%)
  - Ambient light sensor not listed
  - Barometer (low sampling frequency)

- Sensor Fusion
  - Acc & Gyroscope Combo is the best!
  - 74.1%
  - Null (Redundancy & Noises)

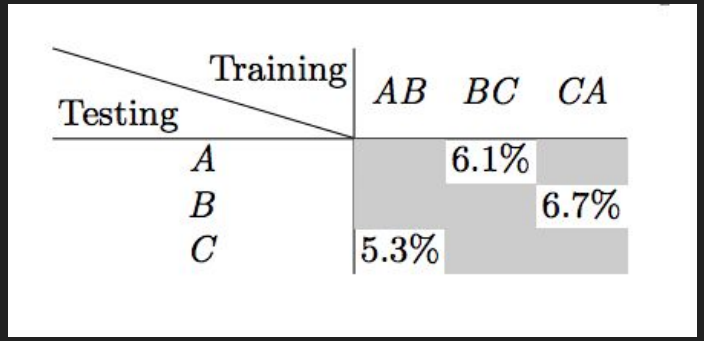


Cross-User Exploitation

- Inclusive cross-user exploitation
- Exclusive cross-user exploitation



Testing \ Training	A	B	C	ABC
A	70.1%			79.6%
B		16.7%		30.0%
C			17.9%	20.5%



Testing \ Training	AB	BC	CA
A		6.1%	
B			6.7%
C	5.3%		

Ways to avoid being attacked

- Use password with longer digits.
- Use Figure Unlock, Face ID, Touch ID.
- Use non-standard numerical keyboard.
- Multi-factor Authentication.

- Do not use common combinations.
- Try not to use the same password

What should have also be done

- iOS and Android should restrict use of their sensors to App developers…
  - iOS 11 improvements
    - Auto Lock
    - Face ID
    - 2FA
- Users should be able to give permission to only trusted Apps.

The sensor problem goes way beyond just a PIN combination…

Location, Behavior, other important private information...

Work Cited

Berend, David, et al. “There Goes Your PIN: Exploiting Smartphone Sensor Fusion Under Single and Cross User Setting.” Open Access, 5 Dec. 2017, pp. 1–19, eprint.iacr.org/2017/1169.

NTU Study Finds That Hackers Could Guess Your Phone PIN Using Its Sensor Data. Edited by Lester Kok, 26 Dec. 2017, media.ntu.edu.sg/NewsReleases/Pages/newsdetail.aspx?news=e57faffc-24ea-4034-9181-f5fea9850690.

Thanks for listening!!

Any Questions?

Ziheng Xu
704756821