Proximity Detection via Deep Learning

Julia Meister
Supervised by: Konstantinos Markantonakis & Raja Naeem Akram
Information Security Group, Smart Card and IoT Security Centre

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The Smart Card and Internet of Things Security Centre

Objectives

To evaluate Deep Learning models as a proximity detection mechanism.

- Design Deep Learning models to test on proximity detection.
- Train and evaluate the models' performance.
- Analyze the results and compare them to previously applied analysis methodologies.

Introduction

Near Field Communication (NFC) has enabled mobile phones to emulate contactless smartcards, which also makes them susceptible to relay attacks [1]. One of the methods proposed to counter such attacks is proximity detection via ambient sensors. Both the payment terminal and the payment device, in this case a mobile phone, measure their environments' characteristics such as the lighting and noise levels, and then compare them to decide whether a transaction is genuine.

We assume that a mobile phone and transaction terminal are in a similar environment (as captured by the sensors) during a genuine transaction because they are physically close together. In contrast, a malicious transaction in the form of a relay attack implies that the genuine devices are further apart, and are therefore likely to be in different environments.

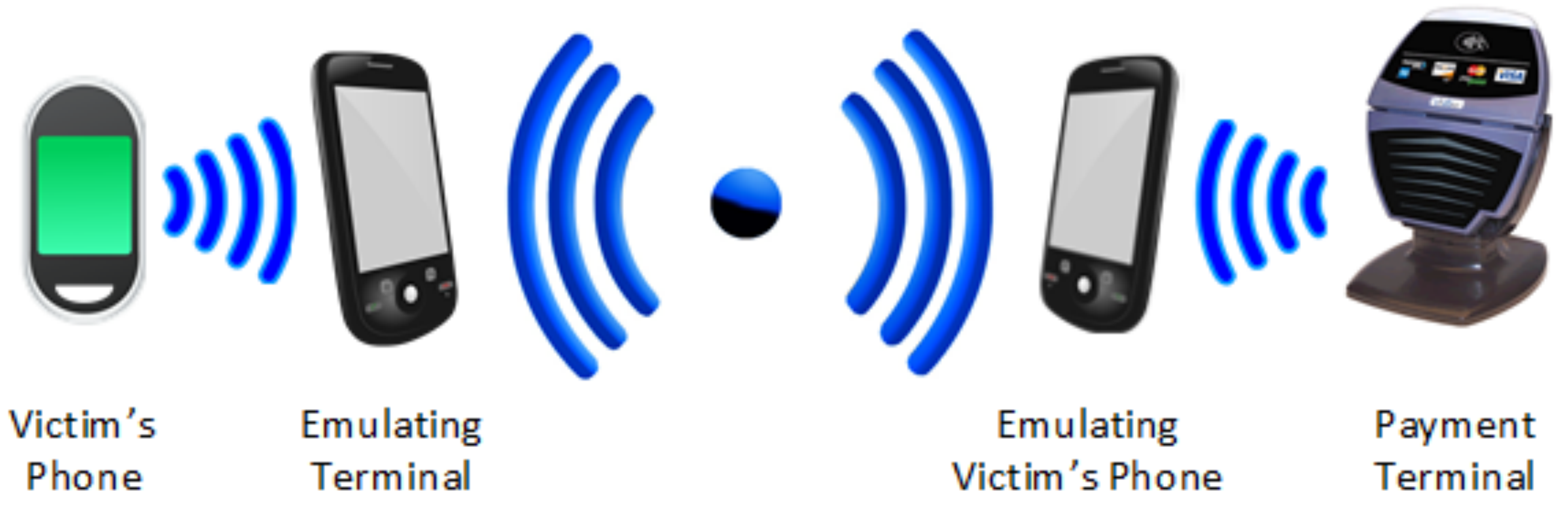

Figure 1: Overview of a Relay Attack

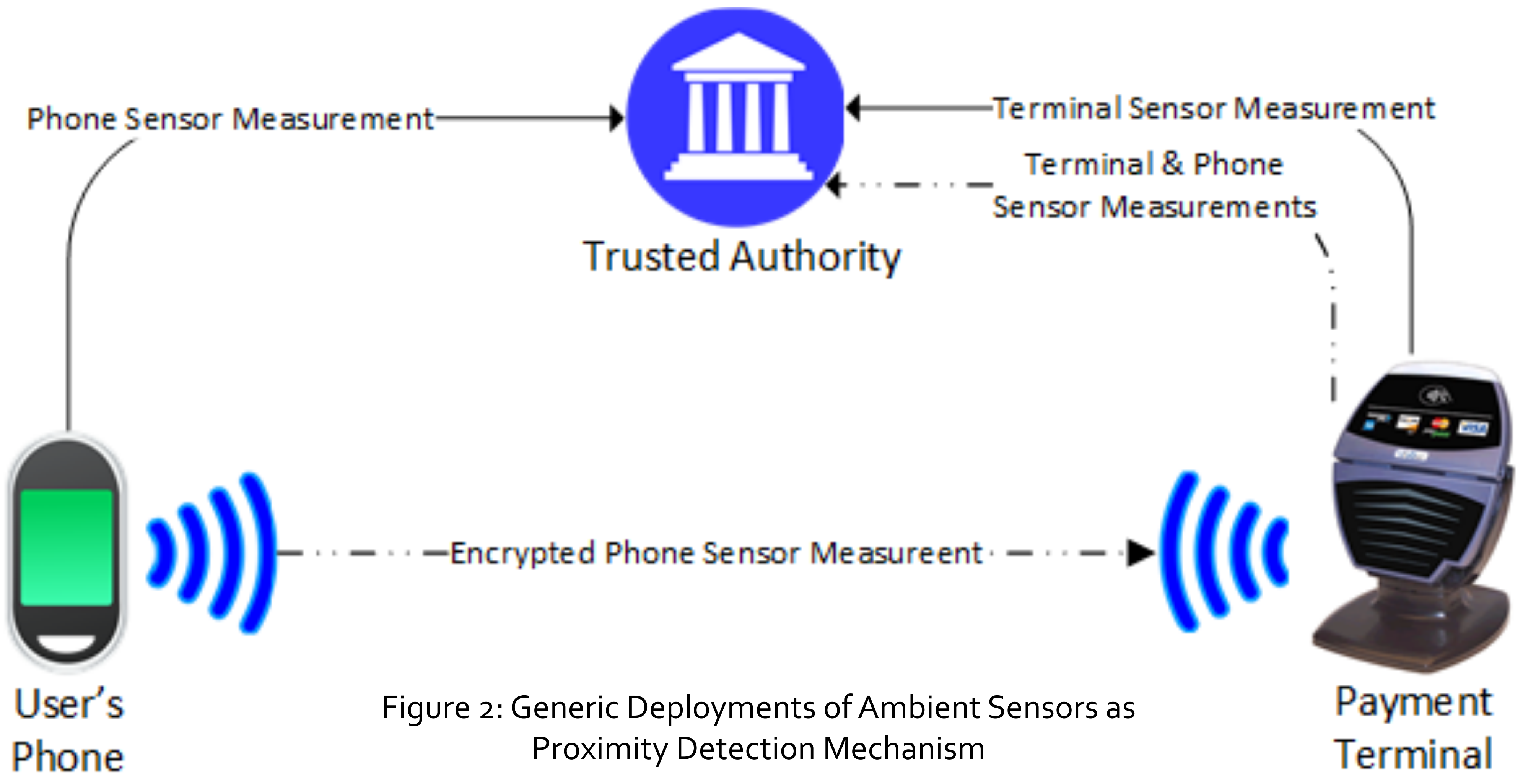
Phone Sensor Measurement
Trusted Authority
Terminal Sensor Measurement
Terminal & Phone Sensor Measurements
Encrypted Phone Sensor Measureent
User's Phone
Payment Terminal

Figure 2: Generic Deployments of Ambient Sensors as Proximity Detection Mechanism

Dataset

The dataset resulted from a previous ISG-SCC field trial and has already been analyzed with threshold-based similarity metrics and Machine Learning techniques.

The data consists of ambient sensor readings taken during contactless transactions between the genuine payment device (smartphone), the payment terminal, and the malicious relay device. Deep Learning (DL) generally performs better with a larger training dataset, so a factorial combination of all sensor readings per transaction was generated and included.

Methodology

Proximity detection can be modelled as binary classification, where the DL model identifies a transaction record as either *genuine* or *malicious* (i.e. a relay attack). To that end, two feedforward networks with supervised training were developed to perform the analysis.

Both models were tested on all datasets. Those that achieved over 65% accuracy were trained again using varying hyperparameter sets, after which an average accuracy was calculated for the best performing model configurations (over 70% accuracy).

Results and Conclusion

Of the designed Deep Learning (DL) models, only a handful reached of the sensor combination/ parameter configurations reached up to 71% accuracy. Most of the remaining configurations had an accuracy of 60-69% after training.

While the performance is slightly higher overall compared to previous methods of analysis (threshold-based similarity metrics and Machine Learning), it is not yet accurate enough to be used in a commercial setting. However, there is a wide variety of DL models that could possibly deliver more positive results (e.g. Deep Belief Networks).

Recorded Sensors

- Accelerometer
- Gravity
- Gyroscope
- Light
- Linear Acceleration
- Magnetic Filed
- Rotation Vector

References

[1] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, *"Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones."* in RFIDSec, ser. LNCS, S. B. O. Yalcin, Ed., vol. 6370. Springer, 2010, pp. 35–49

Acknowledgements

Konstantinos Markantonakis @ ISG-SCC, RHUL
Iakovos Gurulian @ ISG-SCC, RHUL
Carlton Shepherd @ ISG-SCC, RHUL
Eibe Frank @ Dept. CompSci, University of Waiko, NZ
Raja Naeem Akram @ ISG-SCC, RHUL
Keith Mayes @ ISG-SCC, RHUL