6th Sense: A Context-aware Sensor-based Attack Detector for Smart Devices
Paper Review

Shivam Bhat
bhat41@purdue.edu

10/11/2022

Summary

The advent of 5G and IOT Technology has led to the rapid proliferation of smart devices into our lives. Smart devices help integrate and map our physical world to cyberspace through the use of modern sensors, thereby allowing the development of more user friendly and interconnected devices. However the current permission based sensor management system used by these devices has vulnerabilities that could be exploited by bad actors. These malicious agents leverage the fact that such systems focus on specific sensors (Permission imposed sensors) and often use generic sensors API. The authors through this paper present "6th Sense" - a context aware intrusion detection system to tackle such sensor based attacks. The proposed intrusion detection system uses machine learning algorithms to detect malicious sensor behaviour. What separates this system from presently available systems is its ability to correlate various sensor data to user activities; thereby making it contextually aware. The paper performs a thorough analysis by going over existing systems like Semadroid, AuDroid and DARKLY, showing how such security mechanisms are more focused on application level anomaly detection instead of sensor based threats. It further classifies the sensor based attacks into 3 broad categories which are then shown to be accurately detected by "6th Sense" System through its training on real data collected from 50 actual research participants. While the paper is quite thorough in its approach, I found the sensor's conditional independence assumptions for Naive Bayes to be implausible. Further the authors' proposal to use Neural Networks as one of the alternative detection techniques might result in higher performance overhead. The paper, nonetheless, is very much relevant and also the first to propose such a complete security solution for sensor-based attacks, as claimed by the authors. The detailed process, my comments and suggestions are listed in the next section.

Comments

With the rapid advancement of IOT technologies , smart electronic devices including the omnipresent smartphones; smart devices today have become an essential part of our lives. Devices like Alexa, smart home appliances and our phones are today equipped with most advanced sensors. While they provide us great convenience and further thin the divide between reality and cyberspace,

the presence of sensors has opened up novel ways to exploit them. The existing research on the subject matter is focused more on developing application level solutions such as introducing trusted paths on top of existing security mechanisms for information flow control or detecting anomalies and vulnerabilities in code. These approaches fail to effectively detect sensor-based attacks. To overcome such limitations the paper proposes a contextually aware intrusion detection system called the “6th sense”. The proposed system leverages the fact that for any activity that the user performs a different yet unique set of sensors are activated. By correlating the sensor data with activities, it is able to identify if the current use is malicious or not.

The paper does a great job of highlighting the existing threats. We learn how in android only a few sensors like microphone, camera and GPS are considered under it’s permission based access control. This is further exacerbated by “sensor API” which allows apps to get direct access to certain sensors like motion sensors. We also learn how the accelerometer and gyroscope sensors can be used to detect keystrokes, which makes it essential to secure all the different sensors activated in the context of an activity being performed. With the problem at hand, the paper evaluates the model efficacy against threats for android based phones on a dataset generated from the activity of 50 users. The sensor-based threats are broadly classified by authors into 3 categories which are:

1. Triggering malicious app via exploited sensor
2. Information leak via sensor
3. Information theft via sensors

The proposed “6th sense” system leverages machine learning algorithms like Markov Chain, Naive Bayes, Neural Networks etc. to differentiate normal behaviour from malicious behaviour. The advantage of using models like Markov chain is that it's easy to build and deploy on resource limited smart devices. Similarly Naive Bayes fits the requirement very well due to its fast computation rate and small training data requirement. However the assumption of conditional independence of sensor states is not clear and seems to be in contradiction to the “Sensor co-dependence” design assumption made by the author earlier.
While proposing alternative detection ML techniques the paper talks about the potential use of Neural Networks however refrains from discussing the hyperparameters in the given context, which are an essential part of model tuning. Usage of Neural Networks would also lead to a large overhead which might prevent its deployment on resource scarce smart devices.

To evaluate the system, the research, through its 50 research participants, was able to compile 300 sets of data for 6 user activities, each containing 5 min long

data from 9 specific sensors. On evaluating 6 different performance metrics Markov Chain based detection was found to accurately predict 98% of the attacks. In case of Naive Bayes, having 60% threshold value helped achieve 95% accuracy and a F-score of 82%. From the alternative detection techniques proposed, LMT performed the best with an accuracy of 99.97%.

The paper also does a good job of analysing the performance overhead which can often be the limiting factor for using ML models for such low computing hardware devices.The overall overhead was found out ot be less than 4% of the CPU. However the power consumption was found to be as high as 178.33 mW. The paper proposes to not have all sensors remain on for the analysis and observe data while the device is in unlocked status. However this might result in security and privacy concerns. Further different device use have different time windows and device unlock policy which would make this proposal hard to implement.

Recommendations.

The research has a smaller dataset size and could be expanded to more devices and a broader set of activities. The current research focuses on only android devices which due to its inherent open source nature tends to have lenient privacy and security policies. Manufacturers like Apple which build both the hardware and software of their devices have more strict data and security policies. Even in their app stores , they have more layers of checks and balances which often reduces the chances of malicious apps.

The discussion about performance overheads does not speak about the effect of specific ML models. Models like neural Networks are expected to be computationally heavier than simpler models like decision trees. Having such information could be useful in analysis and modifying such computationally heavier models to run on low power usage.

Lastly, the 6th Sense's evaluation process can be expanded beyond the described 3 threats being considered in the paper to make this more encompassing of the various real world threat scenarios.