Poster: StuxMob: A Situational-Aware Malware for Targeted Attack on Smart Mobile Devices

Shams Zawoad (Student)
zawoad@cis.uab.edu
University of Alabama at Birmingham

Ragib Hasan (Faculty)
ragib@cis.uab.edu
University of Alabama at Birmingham

Munir Haque (Postdoc Faculty)
mhaque@cis.uab.edu
University of Alabama at Birmingham

***Abstract*—The availability of a rich variety of sensors in smart mobile devices has enabled today's software to be situationally aware and to learn about surrounding environment. We explore a novel generation of mobile malware, which utilizes this situational awareness and can attack a mobile device carried by a specific person, or people matching with a specific set of criteria.**

The behavior and threat posed by StuxMob is distinguishable from the existing state-of-the-art malware. Today's malwares attack devices either just after the devices got infected or through a command-and-control based botnets. In contrast, StuxMob will launch its payload and perform a specific act against the target, only if it finds a match between a given profile and the person carrying the device; otherwise it remains dormant. By using off-the-shelf sensors of the mobile devices, StuxMob combines the physical activity of users with their surrounding environments to create users' profile. We analyze the feasibility of such a malware and propose defense mechanisms against this type of targeted attack.

I. Introduction

In the past, software used to be confined only to the system on which it was running, with limited situational awareness about surrounding environment or its users. With the introduction of sensor-rich desktop and mobile computing devices, applications now have access to a vast amount of sensory information. For example, using accelerometer and gyroscope sensors, researchers showed that it is possible to identify different human activities [1, 2]. They obtained a high level of accuracy in recognizing some basic actions, e.g., walking, jogging, sitting, and standing. In addition to these basic actions, multiple sensors can simultaneously be used to identify very precise activity. For example, we cannot detect office work on the computer from only the accelerometer sensor data, but by fusing the accelerometer data with the sound data, a mouse click or keyboard typing can be detected [3]. While the activity information can be used for constructive purpose [4], this information can also be exploited by malicious people to launch targeted attack.

Targeted attacks have become one of the most important issues in security community, because of the StuxNet[1] attack on an Iranian nuclear facility. The behavior of StuxMob is similar to StuxNet or Flame [2] malware, but for humans rather than areas or countries. One can think of it as "StuxNet for Human Targets". Once the malware detects it has infected a mobile device matching the profile of its target, then it launches its payload and performs a specific act against the target, devices owned by target, data about the target, or nearby devices/networks. StuxNet or Flame was designed for traditional desktops in mind. As computing gets more and more mobile, we posit that mobile devices such as smart phones are a more lucrative target and can provide a plethora of effective information (and intelligence) in a much better way than StuxNet or Flame.

The threat posed by such targeted malware has a wide range of effect. Other than spying on general people, a targeted malware can identify the people of our interest, and can trigger a spyware only on that particular class of people's phone. For example, a malware that can detect that it has infected the mobile phone of a politician or an Army General, can start eavesdropping on the carrier of the phone and the surrounding areas. In another targeted attack scenario, an attacker can launch a hactivist attack on a specific class of people. Without attacking general people, they can target the employees of a particular organization or only the high official of an organization for their attack. Spammers can also use this malware to show appropriate advertise for a specific group of people, which can increase the chance of alluring victims to visit phishing website. Additionally, exploiting the Bluetooth and Wi-Fi interfaces, the malware can attack the nearby devices. Identifying a specific person and attack on his health is actually possible by using the vulnerability of wireless communication. For example, a malware, which knows that our target wears an insulin pump and finds a profile match with the target, can issue a command for lethal dose to the insulin pump.

The goal of this paper is to demonstrate the feasibility of building a targeted mobile malware using off-the-shelf sensors. Although we are presenting essentially a new generation of attack against mobile devices, the purpose of this work is to keep ourselves ahead in the game against real attackers. Our vision is to motivate fellow researchers to build and deploy defenses before these attacks are actually launched.

The contribution of this work is threefold: (i) explore the feasibility of building personal profile by using off-the-shelf sensors of mobile devices, (ii) identify the threat of abusing sensors' capability to build a new generation of mobile malware for targeted attack, and (iii) identify a set of targeted attacks, and defense mechanisms against those attacks.

[1]StuxNet: http://bit.ly/a2A072
[2]Flame: http://bit.ly/K6wYKf

II. System Model and Approach

A situationally aware mobile malware can be in effect, if the mobile device is always on and with the user, either in pocket, hand, or in parse. Given that modern users heavily rely upon their mobile devices (especially phones), this is a valid assumption to make [5]. The malware is permitted to access the required sensors. As the default Android security model does not protect third party applications to access accelerometer, light, proximity, and other sensors, a malware is permitted to access the sensors.

To build the personal profile of a device owner, we identify different activities, and the surrounding environment of the user during the activities by using the built-in sensors of mobile devices. Then we maintain a log of activities, which contains the starting time and duration of an activity, and information about various environmental features, e.g., light, sound, etc.. From this activity log, we can classify the user to a particular class.

One of the most important features to classify a person is *walking*. Time and pattern of walking can expose the profession of a person. If we observe most of the walking of a person at early morning and after the evening, then we can infer that person as a jobholder, who goes to office in the morning and returns home at evening. But for the students, we can observe a different pattern of daily walk. Students do not go to class at early morning every day. It depends upon their class schedule. We also found that in single day, during regular office hour, students walk much more than a desk jobholder. A person who works at an office seldom moves from his workstation. From the accelerometer and gyroscope data, we can also identify walking speed and height of a person.

Another important attribute is *conversation over phone*. While trying to identify the activity of phone conversation from proximity sensor, we find that the proximity sensor gives same value when the phone is in pocket or a user holds the phone in hand. However, we can use the light sensor value combined with the proximity sensor, and gyroscope to detect the event of phone conversation. With the presence of ambient light, the light sensor can indicate whether the phone is out of pocket or not. The gyroscope can identify the position of the phone, and finally, we can use the proximity sensor value to detect the event of phone conversation. Now, based on the time and duration of phone conversation, we can classify people to different groups. We can also identify a specific person by detecting this event. Consider this hypothetical scenario. Bob is an attacker, who knows Alice's phone number and Alice's phone is already infected by StuxMob. If Bob gives a call to Alice and Alice receives the phone, then the malware running inside Alice's phone can trace this action using different sensors and will notify to command and control (CC) server. If Alice's receiving time and changes of sensor value of her phone coincides, then the CC server will be sure that the malware is running inside Alice's phone and it will send a trigger command to only Alice's phone.

Researchers have explored that we can detect the tap event of the user using motion sensor [6]. With the help of tap event, we can acquire very crucial information about a user. For example, we can identify what the user is typing on his phone. Thus, we can get all the messages or the tweets written by the user. From the messages and the tweets, we can infer about a user's location, age, occupation, gender, activity, and his friend list.

Microphone can also play vital role in building user profile. By using the microphone, we can get the surrounding sounds of a user. Using an appropriate classifier for the frequency, we can distinguish sounds of vehicle, typing on keyboard, music, people chattering, air conditioner, and many more. From these sounds, we can infer about the current environment of the user. E.g., sound of vehicle for a long time says that the user is currently on road, or if we get the sounds of air conditioner, we can say the user is at home or office. From the keyboard typing sound, we can identify how long a person types in a day. From this data, we can infer about the job category of a person.

Future sensors will be more powerful and be able to determine some bodily features, e.g., heart rate, excitement level, and mood, as well as some environmental features, e.g., temperature, humidity, and altitude. With the help of these sensors' data, the malware can identify a person more precisely.

III. Conclusion

Applications running on mobile computing devices carry sensitive personal information that gives them the ability to identify, classify, or generate a profile of the corresponding mobile device user. Hence, a variation of StuxMob aimed for targeted attacks is very much a reality. Unfortunately, there has been no work that addresses the threat of launching a targeted attack from smart mobile device. We take the very first step to explore the feasibility of such a targeted malware using the smartphone sensor data, and propose some mitigation strategies to overcome this attack.

References

[1] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Activity recognition using cell phone accelerometers," *SIGKDD Explor. Newsl.*, vol. 12, no. 2, pp. 74–82, Mar. 2011.

[2] A. Khan, Y. K. Lee, S. Lee, and T. S. Kim, "Human activity recognition via an accelerometer-enabled-smartphone using kernel discriminant analysis," in *Proceeding of FutureTech*, 2010, pp. 1–6.

[3] G. Bieber, A. Luthardt, C. Peter, and B. Urban, "The hearing trousers pocket: activity recognition by alternative sensors," in *Proceedings of PETRA '11*, 2011, pp. 44:1–44:6.

[4] S. J. Preece, J. Y. Goulermas, L. P. Kenney, D. Howard, K. Meijer, and R. Crompton, "Activity identification using body-mounted sensorsa review of classification techniques," *Physiological measurement*, vol. 30, no. 4, 2009.

[5] T. A. Wikle, "America's Cellular Telephone Obsession: New Geographies of Personal Communication," in *Journal of American and Comparative Cultures*, 2001.

[6] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proceedings WiSec '12*. ACM, 2012, pp. 113–124.