State of the Art Technology Resit
Anouk Vreeburg 1700089
Teachers: Joanna Pisarczyk & Rhied Al-Othmani

Using Internet of Things to detect mobile trojan malware and alert the user

words: 1498 (not counting references and title)

PREMISE

Using sensors to detect the presence of trojan virus in a mobile phone and the most effective way to warn the user about it.

SYNOPSIS

Cybercrime victims can come from all walks of life. Perhaps even the victim was unaware of what was happening. Even then, damage may have been done if it were to be discovered. The goal of this project is to raise awareness of the cybercrime issue with the help of IoT. It offers a way to help victims locate these enemies so that an immediate attack can be launched.

CONTEXT

Since the start of the pandemic there has been a rapid increase in digital communication (Monteith, Bauer, Alda, Geddes, Whybrow, & Glenn, 2021). This brings both good and bad side effects, with one of the bad ones being cybercrime. These attacks were able to happen due to one of their greatest weapons: malware. Malware can be defined as a harmful piece of software that was written with the intent of doing harm, to people and their data and devices (Chng, Lu, Kumar, & Yau, 2022). On average, it takes people around 207 days to notice the hint of a breach (Sobers, 2021). Especially trojan malware, which makes up 51.45% of all malware, is a type of malware that disguises itself as a legitimate program, thus can rarely be found (PurpleSec, 2021). One of the two most targeted victims are young adults, as their needs for diversion, entertainment and social relationships make them lacks in protecting themselves online (Kokolakis, 2017). The other regular victim is IoT.

The Internet of Things (IoT) is a system that is able to connect sensors with devices, such as a smart doorbell. These sensors are then able to "talk" to the cloud through connectivity (McClelland, 2016). Because of the constant connectivity to the Internet, and lack of security, IoT has become vulnerable to malware attacks (Valeo Networks, 2021). Despite its drawbacks, IoT offers advantages that might help the malware issue. Ability to deliver, among other things, fast information, quick responses, automation, insights drawn from large amounts of data, excellent communication, and enhanced data quality (Brous, Janssen, & Herder, 2020).

ITERATION 1

I want to first explain why I chose IoT as the technology to solve the problem before I begin this experiment. I started by conducting further research. I immediately discovered that several unknown symptoms, including overheating, a depleted battery, frequent pop-up adverts, and sluggish phone performance, can indicate the presence of malware on a phone (Lishchuk, 2021). Given that malware is challenging to spot with the naked eye, IoT and its sensors can definitely be useful.

This knowledge led me to the idea that mobile phones also include sensors, sensors that might be able to provide information about these invisible indications. To gain a clearer picture, I concentrated on the whole phone after 2012 rather than on particular phone brands. Each phone has its own sensors in each of the three basic sensor categories: motion, environment, and position (Tillu, 2021).

I quickly put two and two together in a table to see if I can leverage a phone sensor that is now available to perhaps detect a virus indicator.

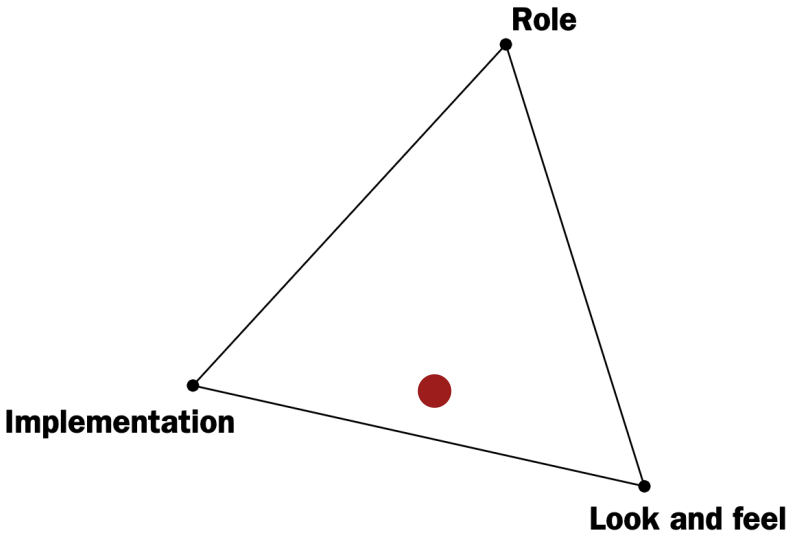
Malware signs / **Phone sensors**	Overheated phone	Pop-up ads	Slow phone performance	Unexplained apps	Surge data consumption	Drained battery	Weird charges	Expensive phone bills	Strange spikes
MOTION Accelerometer (detects axis-based motion sensing)									
Gyroscopes sensor (detects degree of changes in orientation)									
Gravity sensor (detects gravity)									
Pedometer sensor (tracks steps)									
ENVIRONMENT Barometers (detects atmospheric pressure)									
Air humidity sensor (detects humidity)									
Photometers (measures light)									

Ambient light sensor (detects light)									
Temperature sensor (detects battery temperature)									
Ambient temperature sensor (detects temperature)									
POSITION Location sensor (detectes location)									
Magnetometers (measures magnetic fields)									
Proximity sensor (detects presence of an object)									
Finger print sensor (detects fingerprint)									
Face ID (detects face)									

Results indicate that few linkages can be formed. The phone's temperature sensor, however, may be able to gather information about a hot phone. While Chau (2019) notes that "*most smartphones are not equipped with air temperature sensors but they are all equipped with battery temperature sensors,*" the term "temperature sensor" may be deceptive. This temperature sensor can gauge the voltage, condition, and temperature of batteries (Zarkov, 2020).

It's crucial to notify the user about malware after it has hopefully been found. I started the process by asking folks on campus how they would like to be notified in the event of infection. Notifications, alarms, being straight to the point, quick and straightforward, and on a cellphone were the most often mentioned responses.

The scope of this research will lie in implementation and look and feel prototypes (Houde, & Hill, 1997). Implementation prototype focusses on answering technical questions, will an element work towards a goal? Look and feel prototype explores the experience of looking and interacting with an element.

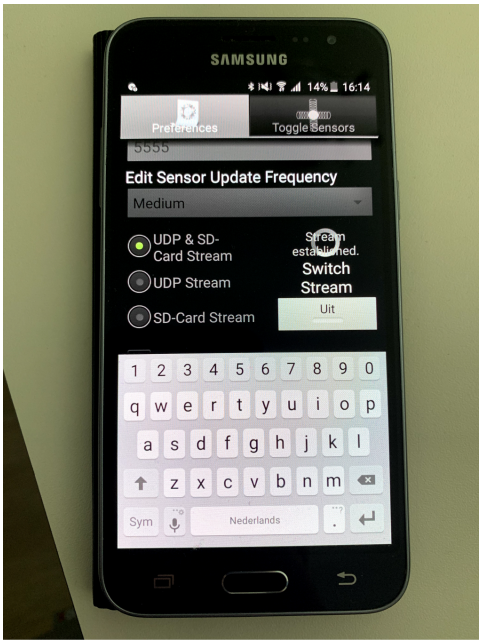


Insights:

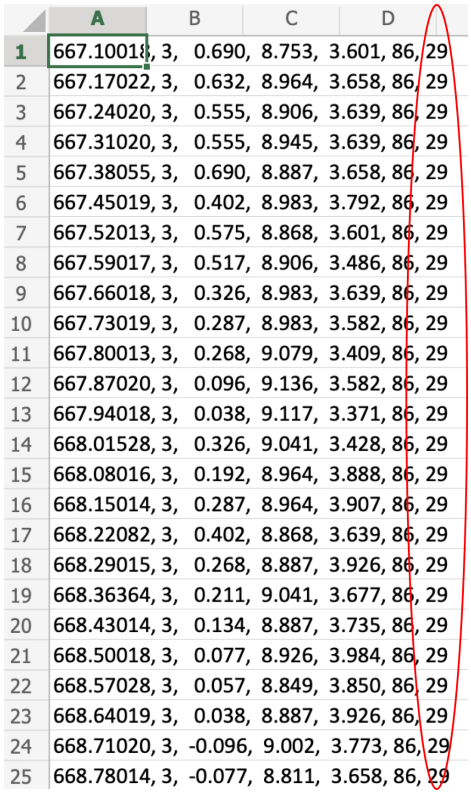
- Find techniques to measure the temperature
- When anything happens to their phone, the majority of consumers want a notification
- Something punchy, succinct, and to the point
- Attention grabbing

ITERATION 2

An old Samsung J3 phone will be used for this experiment. The phone's temperature could only be read with the help of a bridging application. Many applications would not work in the way that I wanted due to the phone's old age. Others could not provide temperature information, then there were also ones that could not share the data, only provided one row of data and or could not continuously update it.



The application Sensorstream IMU+GPS has a compromise. The temperature could be read, and it could provide concise data every few seconds, but not continually. Nevertheless, it transmits a .csv file with data that can be read and utilised in the open-source prototyping platform Arduino with a little assistance. The phone was in a restricted space on each read, unmoved and not charging.

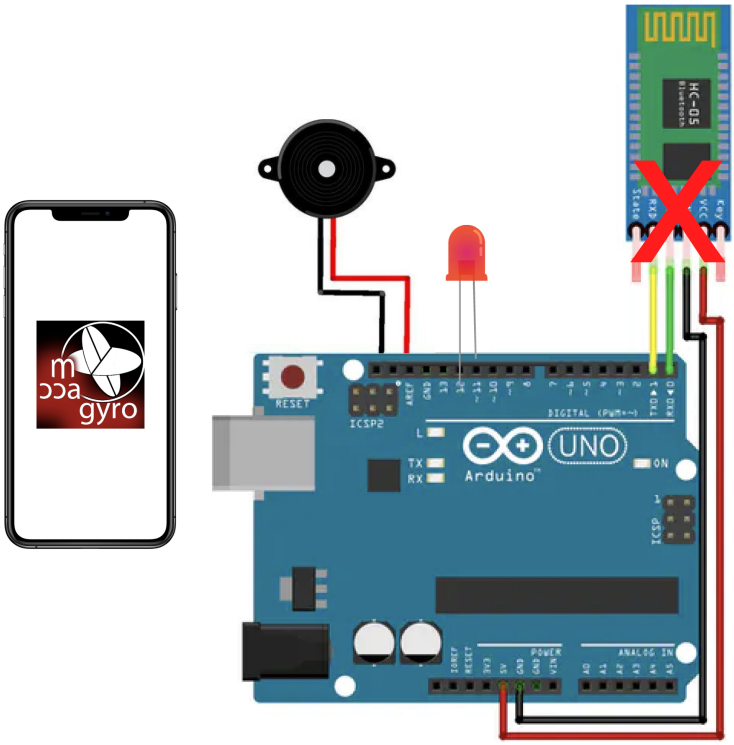


	A	B	C	D
1	667.10018, 3,	0.690,	8.753,	3.601, 86, 29
2	667.17022, 3,	0.632,	8.964,	3.658, 86, 29
3	667.24020, 3,	0.555,	8.906,	3.639, 86, 29
4	667.31020, 3,	0.555,	8.945,	3.639, 86, 29
5	667.38055, 3,	0.690,	8.887,	3.658, 86, 29
6	667.45019, 3,	0.402,	8.983,	3.792, 86, 29
7	667.52013, 3,	0.575,	8.868,	3.601, 86, 29
8	667.59017, 3,	0.517,	8.906,	3.486, 86, 29
9	667.66018, 3,	0.326,	8.983,	3.639, 86, 29
10	667.73019, 3,	0.287,	8.983,	3.582, 86, 29
11	667.80013, 3,	0.268,	9.079,	3.409, 86, 29
12	667.87020, 3,	0.096,	9.136,	3.582, 86, 29
13	667.94018, 3,	0.038,	9.117,	3.371, 86, 29
14	668.01528, 3,	0.326,	9.041,	3.428, 86, 29
15	668.08016, 3,	0.192,	8.964,	3.888, 86, 29
16	668.15014, 3,	0.287,	8.964,	3.907, 86, 29
17	668.22082, 3,	0.402,	8.868,	3.639, 86, 29
18	668.29015, 3,	0.268,	8.887,	3.926, 86, 29
19	668.36364, 3,	0.211,	9.041,	3.677, 86, 29
20	668.43014, 3,	0.134,	8.887,	3.735, 86, 29
21	668.50018, 3,	0.077,	8.926,	3.984, 86, 29
22	668.57028, 3,	0.057,	8.849,	3.850, 86, 29
23	668.64019, 3,	0.038,	8.887,	3.926, 86, 29
24	668.71020, 3,	-0.096,	9.002,	3.773, 86, 29
25	668.78014, 3,	-0.077,	8.811,	3.658, 86, 29

The beginning numbers in the file are made up of the magnetic field, linear acceleration, and rotation vector, which could not be eliminated. The temperature phone is represented by the final two digits. Every second, it reads.

Wanting to alert a notification, I tried sending it from Arduino Uno, through a Bluetooth Module, to the phone. After many tries, it did not succeed, so I decided to take a more creative route.

According to Wogalter, Mayhorn & Zielinska (2016), the majority of individuals typically relate danger to the colour red, warning and caution to the colours orange or yellow, and safety to the colours green or blue. A RGB led resulted as a result. To get the users' attention, a buzzer was also included.



When this was being tested, it would buzz and emit a red light whenever a high number rose. Green light and silence indicate safety. I then put it to the test to see if anyone would want to carry it about.

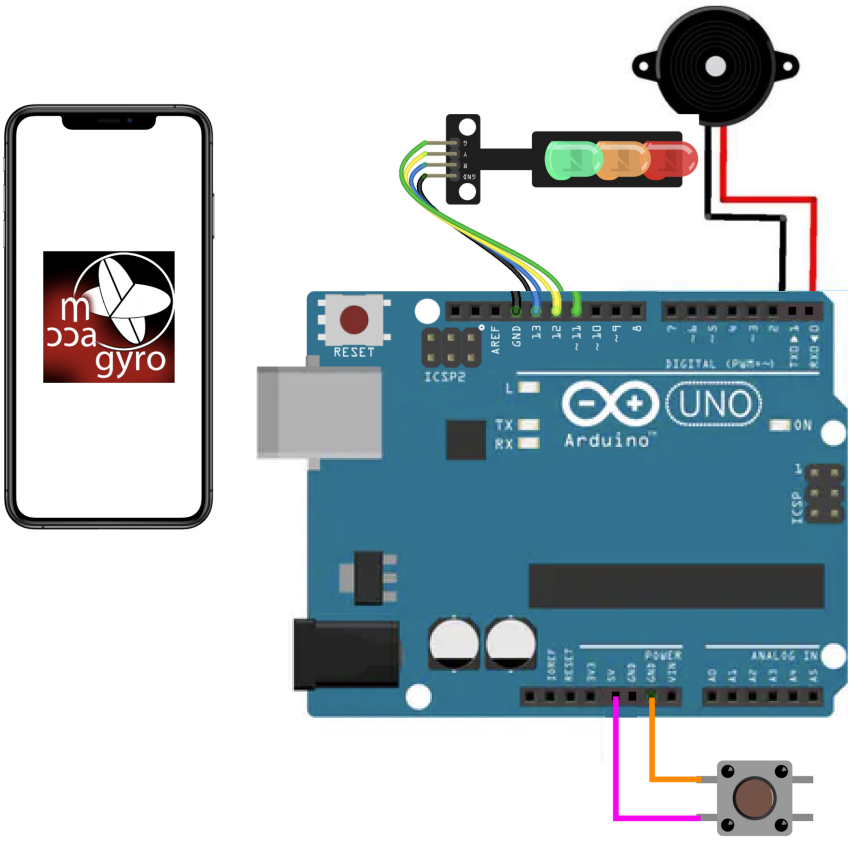
Insights:

- It's crucial to tidy up the file for easier viewing.
- When red and green were illuminated, the user recognised the colour scheme.
- Additionally, there wasn't enough light in the led to see. It was bathed in sunlight.
- Buzzer was very loud! Knowing it may go off at any time, anyplace, made users anxious.
- Making a means for the buzzer to stop and determining when the phone's temperature would rise are both crucial.

ITERATION 3

The normal temperature for a mobile phone is between 25 and 31 degrees Celsius (J, 2022). Anything ranging below 40 degrees qualifies as a normal phone temperature, whereas 40 or above counts as high or too high (J, 2022). After reading the data for multiple days, I made Arduino read through the .csv file and if 31-40 was detected, code orange. If 40 or above was detected, code red. Otherwise, green.

Taking into account user input from iteration 2, a button was added to make it simple for the user to silence the buzzer that signals that the warning was received. The buzzer's pitch has been altered to be less obnoxious, quick, and loud, providing brief beeps to the user. Since the single light was unable to emit a bright colour or provide the colour orange as a warning, it was also replaced with a traffic light. Then it was checked once more.



Insights:

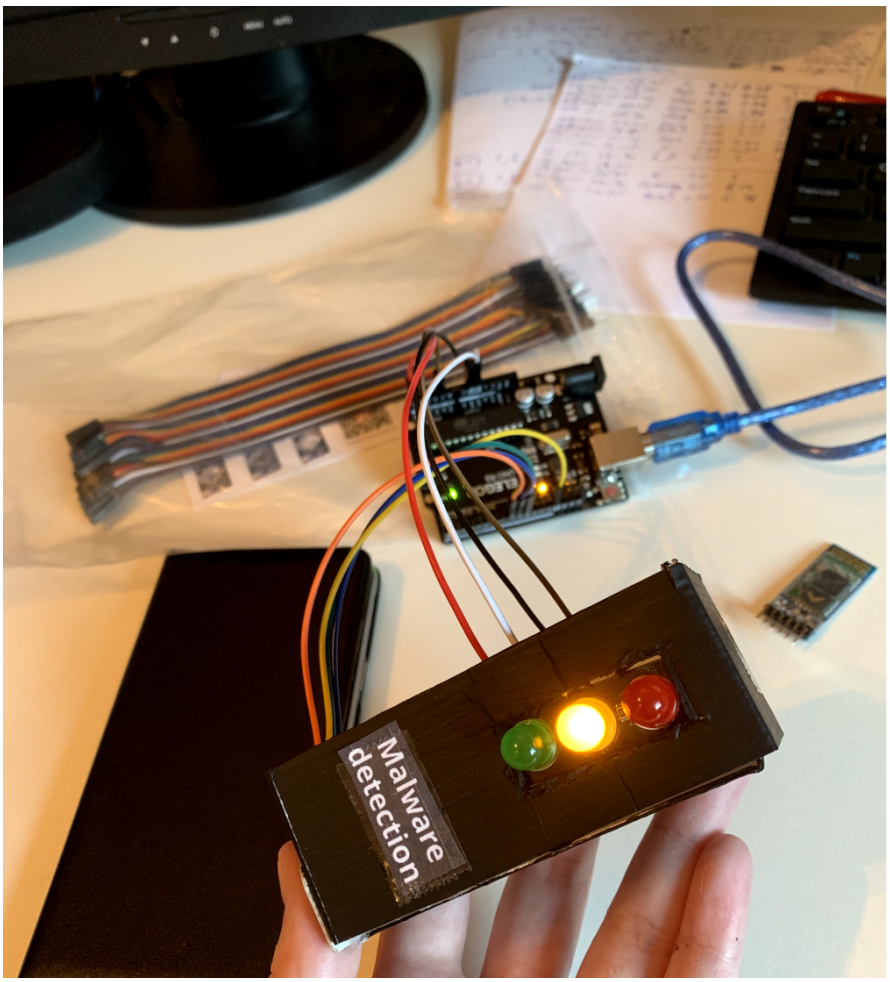
- Should you take into account that the normal temperature can alter with the seasons, and whether it's charging or not? And more? How can you find out?
- The highs and lows of each phone's temperature range can vary, so I might want to search up the old Samsung.
- The buzzer sound was no longer audible outside of a calm room. Find a middle ground.
- The buzzer's constant beep for both colours prevented the user from determining whether the alarm was orange or red.
- Due to the lack of one light on, someone believed it to be broken.
- To ensure that the user is notified nearly quickly, install the alarm at a location, item, or thing that they frequently access.

ITERATION 4

By infecting the old phone with malware, I finally tried to test it out in real life. Gathering information from Reddit posts, https://malwr.com/ and http://www.offensivecomputing.net/ were said to contain malware packages, so I downloaded those. I subsequently went through the .csv file collection process again for a few days.

The results seem underwhelming. Overall, the temperature stayed the same; but, there is some data that indicates that it did increase, albeit not significantly.

The buzzer sound will match the colours more closely after receiving input from iteration 3. A more aggressive sound for a red alert, and a more calmer sound for orange, so the user knows what is happening before they see it. In order to make sure the user knows it is not broken, the light will also consistently shine green when everything is well. The sensors are also placed in a mobile keychain because the user usually always has their phone close by, allowing for instantaneous updates. With the lights in the front, the buzzer in the middle, and the button on the rear, it also appears practical and can be taken off if desired.



Insights

- Sadly, there is no way to determine whether the temperature increase was caused by malware. The phone moved slowly, but due to its age, it already did
- Although it is not always convenient, they loved the functionality of being able to put or remove the keychain.
- Buzzer and light was all good now

CONCLUSION

The implementation prototype experiment obviously needs more testing because it's unclear exactly what caused the one unexpected temperature increase. It is not possible to place all the bets on malware, as temperature rises could have more causes. Receiving a change, though, does inspire hope following malware infection. Additionally, it does bring up some intriguing new queries about how a phone sensor is affected and when malware is most likely to take an action.

The look-and-feel prototype has advanced significantly, moving from a straightforward led and buzzer to a more sophisticated keychain. The prototype became compact, subtle and noticeable. Users can receive timely updates on what is happening. To boost compactness even more, it might be transformed into a mobile widget or notification once the user is through with it. Hopefully, it will function even better in a subsequent study.

REFERENCES

Brous, P., Janssen, M., & Herder, P. (2020). The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, 51, 101952. https://doi.org/10.1016/j.ijinfomgt.2019.05.008

Chau, N. H. (2019). Estimation of air temperature using smartphones in different contexts. Journal of Information and Telecommunication, 3(4), 494–507. https://doi.org/10.1080/24751839.2019.1634869

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 5, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Houde, S., & Hill, C. (1997). What do Prototypes Prototype? Handbook of Human-Computer Interaction, 367–381. https://doi.org/10.1016/b978-044481862-1.50082-0

J. (2022, 11 mei). What Is The Normal Smartphone Battery Temperature? (CONFIRMED-2022). Mobile Tech Addicts. From https://mobiletechaddicts.com/normal-smartphone-battery-temperature/

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lishchuk, R. (2021, 15 juni). How to Find and Remove Malware on Your Android Device. Clario. From https://clario.co/blog/how-to-remove-malware-from-android/

McClelland, C. (2016, 29 oktober). IoT Explained – How Does an IoT System Actually Work? Leverege. From https://www.leverege.com/blogpost/iot-explained-how-does-an-iot-system-actually-work

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4). https://doi.org/10.1007/s11920-021-01228-w

PurpleSec. (2021, 6 augustus). 2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends. From https://purplesec.us/resources/cyber-security-statistics/

Tillu, J. (2021, 7 december). Mobile sensors: The Components that make our smartphones smarter. Medium. From https://medium.com/jay-tillu/mobile-sensors-the-components-that-make-our-smartphones-smarter-4174a7a2bfc3

Valeo Networks. (2021, 10 september). How Is the Internet of Things (IoT) Being Impacted by Malware? From https://www.valeonetworks.com/how-is-the-internet-of-things-iot-being-impacted-by-malware/

Wogalter, M., Mayhorn, C., & Zielinska, O. (2016, 5 April). 18 - Use of color in warnings. Part V. https://www.cambridge.org/core/books/abs/handbook-of-color-psychology/use-of-color-in-warnings/A68E6F7085231D7B06ADA0AEC00CFF03

Zarkov, G. (2020, 17 januari). Can a smartphone measure temperature like a thermometer? Phone Arena. From https://www.phonearena.com/news/can-smartphone-take-temperature_id121600