Tap ’n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens

Seita Maruyama
Waseda University, Japan
maruyama@nsl.cs.waseda.ac.jp

Satohiro Wakabayashi
Waseda University, Japan
wakabayashi@goto.info.waseda.ac.jp

Tatsuya Mori
Waseda University/ RIKENAIP/Japan
mori@nsl.cs.waseda.ac.jp

Sai Ram Varma Budharaju

1. Summary of the paper's findings

1.1. Introduction and context of the study

Smartphones now a days has integrated so much into human lives. They are not only used for internet services but also for monitoring fitness devices, smart homes and contactless payments. Most of the smartphones comes with networking interface features like Bluetooth, Wi-Fi, NFC(Near field Communication). These features enable our smartphone to connect and integrate more into our day-to-day life. Thus, this paper is important to gain knowledge on how vulnerable our smartphones are and some countermeasures to prevent such misuse.

The attack proposed in this paper *Tap ‘n Ghost* aim to attack the touchscreens of the smartphones which has the NFC feature. This attack consists of two attack techniques. “*Tag-based Adaptive Ploy(TAP)*” and “*Ghost Touch generator”* .With these techniques, the attacker can start malicious activities in the victim’s smartphone such as connecting to the smartphone remotely even though victim pressed cancel to the connection. This attack can be easily mounted into the common objects and will be completely stealthy. Though it is possible for a single attack to not work, the attacker will have multiple chances to attack the smartphone.

TAP consists of an NFC modulator which can act in an NFC card emulation mode and can act as a multiple tag. This gives the ability to make tailored attacks on the smartphones like redirecting to a malicious website. Further the webserver fingerprints the device, and this information will be used to make additional tags. Ghost touch generator purpose is to alter the choice of the user that is even though the victim selects cancel it will manipulate the operating system and make it as connect. This is done by injecting external noise signals which create voltage changes and cause the incorrect response by capacitive coupling between the electrodes. This technique combined with information from TAP from fingerprinting the screen. The attacker can take control of the victim’s smartphone.

Attacking the smartphone touchscreen intentionally by transmitting signals to manipulate user choice is mostly new. Unlike the attacks in the previous work The Tap ‘n Ghost attack waits for the victims to arrive at the position and then proceed with the attack. There are a lot of studies on malicious NFC tags which can trigger the smartphone to connect to Bluetooth devices using slightly modified NDEF(NFC Data Exchange Format) tag emulator which can connect to Bluetooth by modifying and sending recorded NFC communication[2]. Another previous work is phishing attack using a smart poster which has malicious NFC tag attached to it. In wall of sheep attack ,Users intentionally scanned the poster with the NFC hoping for discounts and the smartphones are attacked[4].

1.2. Research questions

This paper explored the research question of conducting a more complex and tailored NFC attacks by leveraging NFC card emulation stealthily so the victim will not realize the NFC communications originating from the very common objects like tables. This attack should also control attack parameters by obtaining the smartphone information from fingerprinting for a better success.

This paper also tried to explore the effect of electric field on touch screen which is the basis for the ghost touch generator so that better countermeasures can be developed along with threat to NFC enabled smartphones security. The two novel attacks discussed in this paper solves the problem of mounting very realistic attack on many device models with different configurations.

1.3. Main papers contributions

The main contribution of this paper is to present a class of attacks that can inject malicious functionalities embedded into common objects like tables so that the victim will not realize from where NFC communication is going on. To achieve this ,the paper presents two techniques namely TAP and Ghost touch generator. TAP is to stealthily obtain device fingerprint so that attack parameters can be changed later. Ghost touch generator is to inject incorrect response so that the attacker can get access to the victim’s smartphone.

This paper also presents the technical feasibility of the Tap ‘n Ghost attack. The authors used 24 smartphones for the TAP attack and smartphones for the Ghost touch generator. The practicality of this attack is explained through a survey involving 300 respondents and involved 16 participants whose phones are equipped with the NFC feature. The paper contributed to some of the counter measures to prevent from being attacked by this approach like NFC authorization and some changes to touch screens that can deal with noise interfering with capacitive touch sensing.

1.4. Threat model

The objective of this attack is to perform tailored attacks on the victim's smartphone by attacking the touchscreens of the NFC enabled smartphones through malicious NFC tags embedded inside the common objects so that the attack will be stealthy and by orchestrating this attack the attacker can access the confidential information by targeting the select individuals. We assume that attacker has embedded al the required hardware such as NFC emulator, single board computer and high voltage transformer for ghost touch generator inside the objects like table. Another assumption is that victim has an android phone equipped with NFC and unintentionally places it on the table near to the table where we have the Tap n' Ghost setup. Thus, the smartphone will automatically read the NFC tag and trigger risky action if it is unlocked or not in sleep mode.

Capabilities of the attacker is the equipment required to mount this attack like battery pack, raspberry pi and DDS generator are not very expensive and can also be easily obtainable. The attacker only needs the model of the device so that voltages can be altered accordingly which is done by device fingerprinting by the TAP technique. Another capability of the attacker is he can attack the victim multiple times as long as the smartphone is in the vicinity of the attack setup table. Although this attack is very practical few limitations of this attack are the distance from the NFC tag emulator and the smartphone. Maximum NFC working distance is 3.4 cm so the width of table cannot be too large. The attacks are only limited to phones running on Android operating system.

1.5. Summary of the methodology

To conduct this attack the authors used two attack techniques. First attack is Tag based adaptive ploy in which uses fingerprinting of the device. This uses an NFC tag emulator and a small computer with Wi-Fi controller installed. This technique works with a web server which can work from anywhere if it is connected to the internet. The attacker also needs a power source to control the NFC tag as required for the attack scenario. Firstly, the NFC tag embedded into a table has a tag with the URL data recorded and waiting for the victim to come near it. As soon as the victim's smartphone comes near to it the NFC tag redirects the browser to open the URL. The redirected website uses device fingerprinting and collects the device information and sends it to the onboard computer as the computer has internet access. The computer then determines the suitable tag for the smartphone of the victim and rewrites the NDEF record. Once the new NDEF is read by the NFC of the victim smartphone again and will be under attack again as the NDEF received is new and old one is gone.

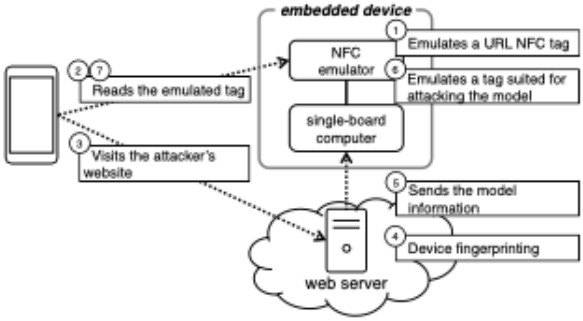

Figure 1: Attack setup of The TAP with device fingerprinting[1].

The authors of this paper came up with the idea of camouflaging the NFC based attack and take full advantage of the NFC stack. This is to mislead victims to make them naturally approve the connection requests that are sent by the attackers. The authors presented two methods one with device fingerprinting and one without it. In this the goal of the attacker is make manipulate the victim to select connect button when a malicious pop us disguised as a normal system notification such as "connect to network" is given. Once the victims tap on connect, the attack is established. To make the attack stealthier the attackers can use the device fingerprinting so that they can leverage the apps that are installed in the victim's smart phone. This is to mislead the victim. That the pop up is a real message that is sent from the installed app.

Ghost touch generator is the second techniques presented in this paper to tackle the problem that if the user did not select yes to the malicious connections. Employing this the attacker aims to cause the malfunction and make the touch of one button as the other by injecting external noise signals. Intentional malfunction can be caused by electric circuit by producing large voltage causing electric field near capacitive touchscreen. .This is done by applying change in current into RX electrodes through capacitive coupling and causing a false touch. So, when a prompt asks the victims to connect to the Wi-Fi with the options as cancel and connect even if the user selects cancel the ghost touch generator changes it as connect and the smart phone is attacked.

1.6. Summary of the experiments and results

The authors of this paper successfully conducted both the attack techniques namely TAP and Ghost touch generator and studied different scenarios and their outcomes for these novel attacks. The paper discussed is an attack paper so the participants in this study do not know the true objective of the test or attack. The participants are selected from the group who volunteered for the study from the university and are not aware of the fact that the tables are embedded with the malicious NFC tags. The experiments are designed in such a way that the participants are treated fairly and designed the attack such that it is non-intrusive. Multiple NFC tags are

embedded into the tables to study the status of NFC equipped smartphones using this the attackers can determine whether the smartphone is locked or not when brought near the table. Ghost touch generator works in the range where TAP works. Among the seven devices on which ghost touch is tested it worked on 5 models causing some disturbance and a wrong touch three models caused the perfect malfunction and there by connecting to the Bluetooth device of the attacker.

The practicality of the threat is tested based on three assumptions. First assumption is if the android phone is equipped with the NFC. The validity of this assumption is the share of android in the OS is 84% which is huge making the target devices number very large and among the survey group of 300 almost 214 people reported that their devices have NFC, and it is forecasted that the devices with NFC will rise by 17% in the next five years when this survey is conducted. The second assumption is that the device should have NFC enabled to attack the touchscreen of the smartphone. The authors investigated the 24 models which they tested and observed that out of 24, sixteen of the models have NFC turned on default in the factory settings. Also, with the rise in usage of online payments will incentivize the users to turn on the NFC feature. In the survey conducted among 214 people with NFC 48 replied that NFC is turned on in their phone always and 11 of them answered they turn it on occasionally.

Device	Manufacture	Android Version	Maximum Reading Distance [cm]	NFC R/W Activated in Factory State	Message Type (Wi-Fi)	Messag (Bluet
ONETOUCH IDOL 2 S	ALCATEL	4.3	3.0		—	BT-EN
Nexus 7	ASUS	6.0.1	4.0	✓	WI-EN-1	BT-EN
SAMURAI KIWAMI	FREETEL	5.1	3.0		WI-EN-1	BT-EN
ARROWS NX F-05F	FUJITSU	5.0.2	4.0		WI-EN-1	BT-EN
Nexus 9	HTC	7.0	4.5	✓	WI-EN-1	BT-EN
INFOBAR A02	HTC	4.1.1	2.5		—	BT-EN
Ascend P7	HUAWEI	4.4.2	3.5	✓	—	BT-EN
TORQUE G02	KYOCERA	5.1	3.5	✓	WI-EN-1	BT-EN
TORQUE G01	KYOCERA	4.4.2	3.5	✓	—	BT-EN
Nexus 5X	LG	6.0	4.5	✓	WI-EN-1	BT-EN
isai vivid	LG	5.1	5.0	✓	WI-EN-2	BT-EN
DM-01G	LG	5.0.2	5.0		WI-EN-2	BT-EN
ELUGA P	PANASONIC	4.2.2	2.0		—	BT-EN
Galaxy S7 edge	SAMSUNG	6.0.1	3.0	✓	WI-EN-1	BT-EN
Galaxy S6 edge	SAMSUNG	6.0.1	2.0	✓	WI-EN-1	BT-EN
Galaxy S4	SAMSUNG	5.0.1	3.0		WI-EN-1	BT-EN
AQUOS ZETA SH-01H	SHARP	5.1.1	3.5	✓	WI-EN-1	BT-EN
AQUOS ZETA SH-04F	SHARP	5.0.2	3.5	✓	WI-EN-1	BT-EN
AQUOS SERIE	SHARP	5.0.2	3.0	✓	WI-EN-1	BT-EN
Xperia XZ	SONY	7.0	3.0	✓	WI-EN-1	BT-EN
Xperia Z5	SONY	6.0	3.0	✓	WI-EN-1	BT-EN
Xperia Z4	SONY	6.0	4.0	✓	WI-EN-1	BT-EN
Xperia Z3	SONY	5.0.2	3.0	✓	WI-EN-3	BT-EN
Xperia Z2	SONY	5.0.2	2.5		WI-EN-3	BT-EN

Figure 2. Practicality success rate of the threat from the study conducted by authors[1].

The third assumption is the validity of human behavior. To test this tables in libraries and café are equipped with embedded NFC tags and the participants are made to work in the environment. Smart phones are used for many purposes and the participants do not know the attack methodology while this study is done for the fair and transparent results and in consideration of their privacy a non-intrusive attack is conducted which says whether the phone is locked or unlocked. This survey is done o 16 participants with NFC enabled android smartphones are designed various scenarios.16 NFC readers are embedded into the tables and connected to the laptop and when the smart phone is put on the table it reads the NFC tag and determines whether the smartphone is attackable or not by checking if the smartphone is locked or unlocked.

Further the study procedure for this attack consists of three sessions. They are asked to participate in a quiz session, break and a debriefing of the attack session. In the quiz session all 16 participants provided an opportunity to attack their phone as they unlocked their phone and brought it near the NFC, In the second session 10 out 16 participants presented opportunity to attack and 2 of them were using their phone far from the table. None of the participant knew about the secret setup of NFC tags in the table Thus making this attack stealthy and all presented opportunities making this attack very practical.

Lastly, Authors also presented the success probability of the single attack under the ideal attack conditions ,the success probability is determined on all the assumptions and their success rates, so the single attack success probability is 0.03.Although this is not high, the attacker has the opportunity to attack the smartphone multiple times. With this setup installed in public places the attacker can target as many users as possible who take that seat. The success rate increases if we consider the attack as success if the attacker can attack at least one phone in a duration of time. Attacker can also increase the number of cycles of ghost touch generator for 3 times the success probability is at 0.71 and the number of tables can be increased if they want to speed up the successful attacks.

The paper also presents the results of these attacks in different attack scenarios. Attacking random targets if the attack set up is in the public places like libraries or café so that the attacker can have as many users which will lead to increase in the success rate of the attack to almost one as the time increases. As the number of attacks increase the rate of success for this kind of attack also increases linearly with time. The second attack scenario is attacking the specific targets. In this case the attacker will set up the malicious table in a certain spot where the target is likely to come rather than in a public place. Here even though the success rate is low even one single attack can have more value as the attacker can get access to the confidential information and can impersonate to launch a more advanced attack. Though the success rate may be low over a long time the attack will succeed and the attacker objectives can be achieved.as he will have several opportunities to attack the target over a long time. The authors of this paper tested all kinds of scenarios and presented a careful; study of how practical and stealthy this attack is which is very successful and presented some countermeasures to protect against these attacks like adding

extra authorization and proposing changes to the touch screen technology.

2. Main takeaways and limitations of the work

2.1. Major takeaways

This paper proposed a proof-of-concept attack which is capable of injecting functionalities which can trigger risky actions on the smartphone of the victim. The key takeaway is this attack has a very high chance of success as seen from the results of the user study and online survey. The participants didn't notice that their smartphone is being attacked until they were told because of the embedded NFC tags within the common objects. So, the attack is very stealthy and can be done so many times without victim noticing.

Implementation cost of this attack is roughly 490 USD which is very much affordable given the success rate and the capability of this attack. Cost for this attack is mostly to purchase NFC readers so if the attacker wants to perform the same attack at a lower cost it is very much possible as most of the cost is for NFC. This attack can be mounted with a smaller number of NFC tags and can still be successful. The hardware used for the attack is reusable, so the attacker need not invest more money whenever he wants to mount the attack.

The proposed attack works in practice as seen from the studies. The participants all gave the opportunity to the attacker to attack and are unable to notice any NFC tag which makes attack very practical in the real world. This attack can be done in public places as well as target certain people to access confidential information which can harm the victim and can be attacked multiple times without even knowing that he is being attacked. Thus, making this attack very much doable and practical.

Though the attack is very successful ,the paper presented some countermeasures to prevent these kinds of attack such as authorization for NFC like in operating systems like IOS that performs NFC operations only after authorization is provided. Manufactures should come up with technology to deal with external noise interfering with touchscreen controllers so that attacks through ghost touch generator can be prevented. There are some digital and analog technologies already in market that can filter the external noise and thereby preventing wrong inputs.

2.2. Major limitations

The limitation of this paper is that the attack is only restricted to android devices. This attack techniques proposed in this paper will not work for other operating systems like IOS as it needs authorization for the NFC tag to trigger any action. This prevents the attacker from attacking a person who do not use android phone. Though majority of people use android devices attacker cannot target certain people and achieve success if they are not in the victim attack spectrum.

The attack range of the technique is relatively small as the maximum reachability of NFC in a practical world is low. Though it says NFC can be read from 20 cm but in reality it can be read from a maximum of 5 cm. So, when the NFC tag is attached to the table the maximum communicable thickness for the wood is 5mm.The maximum communicable distance at average for success case ids found to be 3.4 cm which means the user has to almost place the phone on the table and very near to the tag.

Using Ghost touch generator sometimes even though a false touch is generated it does not mean it generated a desirable touch that is ideally it should change our touch in cancel to connect but few times the touch will just be unresponsive. If there is no response for 5 consecutive touch the attack is considered as an unsuccessful attack. Among the devices studied few devices are unresponsive and few devices generated false touch but not the desired touch.

Final limitation proposed in this paper is the counter measures which says that android operating system should ask for authorization of the user for NFC actions, but this will reduce the usability and flexibility of the NFC. The counter measure proposed is to detect the embedded physical NFC tags which is not scalable as it needs so much of inspection of many common objects.

3. Fundamental previous work

3.1. Practical Attacks on NFC Enabled Cell Phones

Published in 2011

Roel Verdult
Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands.
rverdult@cs.ru.nl

Franois Kooman
SURFnet B.V., The Netherlands.
Francois.Kooman@surfnet.nl

3.2. Research problem

This research problem for this paper is to come up with a practical attack that can make a Bluetooth connection without user authorization and trigger the mobile device to install malicious software which can spread viruses across the device. The aim is to install an application that has no access limitations and do need any authorizations for the advanced and security features like access files, contacts and some GSM features.

This paper also aimed to analyze the security vulnerabilities of an NFC feature enabled mobile phone. This paper analyzed the vulnerabilities in content sharing and NFC Bluetooth pairing compatibilities in a Nokia phone which

used a pin passing mechanism making it vulnerable once the secrecy of cipher is lost.

3.3. Main contributions of the work

This paper analyzed and demonstrated practical attacks on the NFC features phones on the latest framework at the time of writing this work Nokia 6212 classic. The proposed work focused on Nokia proprietary features like Content sharing and NFC Bluetooth connection and showed communication between the Nokia phone and NFC tag. The attackers are able to send a slightly modified message to the device which could trick user to read faulty tag emulator.

Secondly , the paper analyzed the communication between two NFC enabled phones in which one phone tries to send an object and has ability to impersonate itself as a initiating phone so that it can activate am incoming Bluetooth channel on the target phone. This will enable the attacker to install the install application on the phone without any consent or authorization. This will give the application unlimited access and can install viruses which can be spread to other NFC devices from this device.

3.4. Correlation with the presented work

The proposed work is given as the reference in the main paper for employing tag based adaptive ploy which is injecting malicious functionalities to trigger unwanted risky actions. This reference paper does the same thing. The phone with NFC tag is attacked with help of a slightly modified NFC message and tricking the user to read the NFC tag thus establishing a connect between the Bluetooth devices.

In the main paper attackers employed an embedded NFC emulator tag and tried to send a popup or trigger an action to do a risky action. The reference paper employs the same technique of manipulating the user think it's a genuine tag and thus getting access to the device.

In both the papers once the attackers got the control of the device, they trigger few more activities that can install malicious software which will give unrestricted access to all the functionalities and data of the victim's phone there by impacting the security of the device. This reference paper acts as a basis for the TAP attack conducted in the presented paper.

2.5. A testbed for modeling and detecting attacks on NFC Enabled Mobile Device - published in 2015

Kimberly Gold, Sachin Shetty, Tamara Rogers
Tennessee State University
Nashville,United States.
kgold@my.tnstate.edu
sshetty@tnstate.edu
trogers3@tnstate.edu

2.6. Research problem

This paper solves the research problem of developing experimental testbeds which will model different attack scenarios and detect the threats for the normal payments which will evaluate the successful ghost and leech attack, phishing and steganographic malware attacks.

2.7. Main contributions of the work

This paper the various attack vectors on the mobile payment and payment systems. The attacks are designed and executed in a controlled way were attack vectors were generated based on the scenarios to analyze the security threat and vulnerabilities at the protocols while establishing connections.

Three attacks are proposed in this paper namely Ghost and leech attack which is a relay attack, Phishing attack and stenographic malware attack. This paper analyzes and conducts these attacks in the NFCSec lab to provide experimental platform to assess the impact of the threat on the devices supporting NFC and discussed the NFC tag vulnerabilities.

2.8. Correlation with the presented work

This paper uses the attack of card emulation of NFC tags which is the main principle behind the Tag based Adaptive Ploy. In this paper a phishing attack is implemented using a NFC device and poster with has malicious NFC tag embedded in it. This paper is one of the references which gave the idea of embedding NFC tags into common objects.

This attack has a poster with malicious NFC tag that sends a tailored social media website, and a database will be created to store the stolen credentials. Once the attacker has the credentials the user will be redirected to the app but will never know his credentials are stolen. TAP also almost employs a similar approach but asks for a Wi-Fi connection or pop up to use Bluetooth similarly like in this paper.

Both the papers used the NFC tag card emulation technique to make the user believe that it is a genuine request and gained access to the device. These attacks have the ability to redirect the user to harmful websites and can install harmful software without any consent from the victim.

4. Proposed defenses

4.1. Improving user approval for NFC

One of the defenses proposed in this paper is improving the user approval process for NFC emulation tags. At present the NFC used in the android operating system do not need any additional authorization to launch the applications that are recorded in the NFC tag. Attackers take advantage of this and conduct the attacks by injecting malicious tag recordings without the consent and knowledge of the user.

Android devices should come with a user approval process like the apple operating system is implementing. The proposed techniques do not work on iOS devices because of continuous feedback of authentication requests by the

software. This helps in increase the security of the NFC based activities. Though the convenience of using NFC will be slightly reduced because of continuous authentication it will add more security to the NFC based operations.

To further reduce the risk of attack the android OS should have to modify the way pop messages with NDEF related to NFC should appear and prompt the exact reason why the pop up or action is invoked which will help identify the attacks.

4.2. Advantages of the defense if implemented.

The defense proposed is very easy to implement as it can be done via software update. The update to the software with extra authorization protocols can be distributed over the Air update and can be easily accessible to the users of the smart phones.

The implementation is relatively less expensive and logistically very feasible as we only have to incur costs for developing new software while distributing the software is over the internet and can be accessible by everyone. This defense can immediately protect the user from such attacks.

4.3. Noise filtering

The attackers can cause intentional malfunction of a touchscreen by injecting external noise by producing large altering voltages. To overcome a new defense which has the capability of filtering the noise when it reached a particular threshold so that the mechanism will calculate the waveform and employs an active noise cancelling mechanism.

This defense proposes to have sensing and compensating mechanism so that the sensors will keep on look for the external noise and whenever it is detected the compensating mechanism will calculate and generate the waveform with the similar frequency of and the external noise wave and feed it to the wave form.

The produced waveform will filter the external noise using the adaptive filtering mechanism and reduce the impact of injected noise so that the attacker's noise will have no impact on the working of touch screens thus providing security against Ghost touch generator

4.4. Advantages of the defense if implemented.

The proposed defense does not need expensive hardware as most phones come with amplifier though it needs some changes in its configurations. This solution when implemented can prevent any kind of attack that uses injecting noise to disrupt the touchscreen.

This defense proposed already exists in many media devices, so it need not be developed from the beginning making it easy to implement for the future smartphones that comes with NFC feature.

5. Proposed follow-up research idea

5.1. Follow-up research idea description

Touch screens are becoming the interface between the humans and all the appliances' humans use like smart doorbells, clocking in and out of work and entering corporate offices, ordering food ,public transport tickets etc in the restaurants. Most of these are now a days using touchscreens to provide passwords, pins etc.,

The idea is to propose denial of service attack and a counter measure to the attack. Most people when they leave for the work they usually must clock in their hours and clock out whenever they are leaving and also smart door systems which need us to type the pin in the console in order for the doors to open to get access. The idea is to implement a multiple ghost touch generations on the devices at the same time continuously when the user is attempting to get access so that he will be allowed to open his home or entering the office.

The attacker will continuously send external noise generating multiple touches at the same time so that the input will never be a correct input there by denying the entrance to this home. This will make the user vulnerable as he will be at loss either financially or encounter security issues.

The second part of this research idea is to also propose a counter measure in the form of active noise cancellation which is already used in the multiple premium audio devices which will filter all the external noise using adaptive filtering techniques.

5.2. Research questions

The proposed idea wants to solve the research question of implementing multiple ghost attacks at time and implement a denial-of-service attack which will restrict the user from accessing home and office on time by injecting multiple external noises creating a voltage difference and disrupting the touchscreen function.

The other research question is to come up with a novel defense that can act as a noise cancelling mechanism using adaptive filtering to mitigate the external noise disrupting the function of the touchscreen.

REFERENCES

[1]. S. Maruyama, S. Wakabayashi, and T. Mori, “Tap ’n ghost: A compilation of novel attack techniques against smartphone touchscreens,” in Proceedings of the 40th IEEE Symposium on Security and Privacy (SP). IEEE, 2019, pp. 628–645.

[2] R. Verdult and F. Kooman, “Practical attacks on nfc enabled cell phones,” in *Near Field Communication (NFC), 2011 3rd International Workshop on*. IEEE, 2011, pp. 77–82.

[3] C. Mulliner, “Vulnerability analysis and attacks on nfc-enabled mobile phones,” in *ARES*, 2009, pp. 695–700.

[4] Wall of Sheep, “Nfc security awareness project,” http://www. wallofsheep.com/pages/nfc- security- awareness- project, 2013.