World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:9, 2022

Facilitating a Cyber-Enabled Fraud Using the O.MG Cable to Incriminate the Victim

Damola O. Lawal, David W. Gresty, Diane E. Gan, Louise Hewitt

***Abstract*—**This paper investigates the feasibility of using a programmable USB such as the O.MG Cable to perform a file tampering attack. Here, the O.MG Cable, an apparently harmless mobile device charger is used in an unauthorised way, to alter the content of a file (an accounts record-January_Contributions.xlsx). The aim is to determine if a forensics analyst can reliably determine who has altered the target file; the O.MG Cable or the user of the machine. This work highlights some of the traces of the O.MG Cable left behind on the target computer itself such as the Product ID (PID) and Vendor ID (ID). Also discussed is the O.MG Cable's behaviour during the experiments. We determine if a forensics analyst could identify if any evidence has been left behind by the programmable device on the target file once it has been removed from the computer to establish if the analyst would be able to link the traces left by the O.MG Cable to the file tampering. It was discovered that the forensic analyst might mistake the actions of the O.MG Cable for the computer users. Experiments carried out in this work could further the discussion as to whether an innocent user could be punished for the unauthorised changes made by a programmable device.

***Keywords*—**O.MG Cable, programmable USB, file tampering attack, digital evidence credibility, miscarriage of justice, cyber fraud.

I. Introduction

MOBILE devices such as smartphones, tablets, smart watches, laptops have become a part of our everyday life. These mobile devices cannot function for so long without being recharged, hence the need for a charging cable, or a more generalised term 'a charger'. Seeing chargers or charging cables have therefore become a norm, and they were never really considered security threats or suspicious in anyway as their purpose had always been for charging and in some cases, data transfer. Bring your own device (BYOD) comes with its security risks but the experiments in this paper indicate users, and organisations should now consider as part of their security policies, concerns about bringing your own charger (BYOC). In the past, the most common security concern of users was to avoid downloading malware from the internet, or avoid transferring malware from a computer to their thumb drives or vice-versa. Now, there are mobile device chargers or charging cables also to be wary of regardless of how innocent, harmless, and passive they might appear on the surface. People are less suspicious of power banks and charging cables as they do not consider them IT devices. This lack of suspicion enables them to use almost any free USB ports or cables available without worrying [1].

In this paper, the threat of a forensic evading file tampering attack is considered. The target file represents a record of accounts paid for a small organisation, and the aim of the attacker here is not to incriminate another user but to cleverly alter the content of the file for personal gain; in a subtle way that will not arouse suspicion. In such a scenario, if the fraud is discovered, it calls into question who or what would the blame be attributed to. There are various scenarios that give effect to the outcome of this experiment. For example, an employee could be unjustly punished (fired or even prosecuted) for modifying the accounts record if the unauthorised changes are discovered perhaps during a financial audit or if the account is not adding up. This could lead to different assumptions such as an accountant has colluded with someone else to defraud the company or embezzle money in some way especially if there is evidence that leads an employer to believe the user carried out the actions. The approach used in this experiment is also applicable in scenarios involving student results where a student makes unauthorised modification to their, or anyone else's grades.

It would be unfair and indeed a potential miscarriage of justice for an innocent employee or computer user to be punished for unauthorised actions they are not responsible for.

II. Literature Review

There are three main components of Digital Forensics: the proactive digital forensics, active digital forensics and reactive digital forensics as proposed by [2]. Proactive Digital forensics is implemented before a cyber incident takes place. Active digital forensics is done while the incident is happening, and reactive digital forensics is concerned with investigating after the incident has occurred but could also kick off while the incident is happening [2]. Taking into account the digital forensic components proposed by [2], the experiment and forensic investigation carried out in this paper would fall under the reactive phase of digital forensics as it is carried out after the incident has occurred.

Apart from charging cables, there are also charging ports to be wary of. Kumar [1] talked about Juice-Jacking which is a type of attack that would typically involve a charging port that

D. O. Lawal is a member of the iSEC Research group, and a post graduate research student at the University of Greenwich, London. SE10 9LS UK (e-mail: D.O.Lawal@gre.ac.uk).

D. W. Gresty is a senior lecturer with the School of Computing and Mathematical Sciences at the University of Greenwich, London (e-mail: D.W.Gresty@gre.ac.uk).

D. E. Gan is an associate professor with the school of Computing and Mathematical sciences at the University of Greenwich, London and also the director of the Missing Persons Investigation Unit (e-mail: D.Gan@gre.ac.uk).

L. Hewitt is the Director of the Innocence Project, London and senior lecturer with the School of Law at the University of Greenwich, London. (e-mail: Louise.Hewitt@gre.ac.uk).

also has data connection capabilities. Hackers leverage this by attaching malicious charging cables to public USB outlets so they can steal sensitive data such as credit card data, passwords, or plant a ransomware. Kumar [1] identifies two types of Juice-Jacking: Data theft and Malware Installation. Data theft involves stealing data from the connected device while charging it at any of the infected or malicious charging stations. Crawlers can also search the connected device for sensitive data such as credit/debit card data within a very short space of time (in seconds). Malware installation involves a transference of malware onto the connected device. The installed malware could provide the attackers with access to the victim's locations, pictures, and videos, call logs and even ongoing processes. Categories of malware that could be installed on a victim's device include adware, spyware, ransomware, trojans crypto miners.

Dean et al. [3] discuss the possibility of using Juice-Jacking in identity theft. Identity theft is the use of an individual's personal information without the individual's permission and Juice-Jacking is one of various methods used to steal victims' identity. Juice-Jacking is usually achieved by gaining access to a mobile phone while it is supposedly charging. Malicious code is injected into the device to either steal data or perform other malicious operations by taking advantage of the charging cable which might also have data transfer capabilities [3]. Loe et al. [4] investigate Human Interface Device (HID) attacks and Juice-Jacking attacks. Juice-Jacking attacks can steal data and manipulate a target device by leveraging the mobile access permission while charging [4]. Loe et al. [4] designed and implemented an installation-free security tool named SandUSB, that can scan and monitor attached USB devices to detect if any of the connected devices are malicious or detect if there is a mismatch in the kind of device they have registered as, and what they really are. SandUSB is able to defend against HID attacks and Juice Jacking attacks [4]. The developed tool, SandUSB could be used as a proactive cyber security approach and is useful in defending against malicious USB attacks; however, this typically would not be considered normal for forensic investigations that take place after an incident occurs. Malware that infects USB devices often take advantage of the USB auto-run feature which is disabled in the Windows 10 Operating system, but disabling this feature is still not effective against HID attacks [4].

HID attacks and Juice-Jacking attacks are quite similar and may even be able to carry out certain similar attacks. However, Juice-Jacking seems to be more about taking advantage of the vulnerabilities on the mobile side (iOS and androids) and not really about attacking the PC. The mobile phones are infected when connected to a malicious USB charging port, perhaps while charging or when connected to a USB port on an infected computer.

With the O.MG Cable, the cable itself does the infection or performs the malicious actions and not the port to which it is attached. The mobile device end of the O.MG Cable does nothing but charging and normal data transfer, but this is just to make the decoy more believable and less suspicious. HID attacks send commands to the device they are attached or plugged whereas Juice-Jacking injects malicious code or data to a mobile device while charging at a malicious kiosk or infected port. Furthermore, because of the data transfer capability of the O.MG Cable, it might be possible to use it for Juice-Jacking attacks as well; however, ideally, attacks carried out using the O.MG Cable would still fall under HID attacks because the mobile side of the cable really has nothing to do with its operation. Moreover, the O.MG Cable is used also to send commands to a computer through the computer's USB port. The O.MG Cable is like a wireless and more flexible version of the Rubber Ducky [5]. The O.MG Cable is more flexible in the sense that it can be used to send commands and keystrokes on the fly; codes can be modified, stored, and loaded on the fly without having to disconnect and reprogram the device. The O.MG Cable has a remote interface that can accept the code from any device that can connect to its wireless signal. With the Rubber Ducky, one would usually need to unplug to reprogram, and re-encode the payload in binary, then reload onto the Rubber Ducky before it can run a different command, but this is not the case with the O.MG Cable. There is a micro-controller embedded within the O.MG Cable and one might not be able to differentiate the O.MG Cable from a regular USB charging cable [1].

In relation to programmable devices being used to carry out actions like a human user, [6] used the Rubber Ducky to perform a framing attack where false incriminating evidence were planted on the victim's machine to make it appear like the victim had performed those actions. The evidence planted in [6] were false web history, file download of the type that would be seen in investigations of indecent pictures of children which are punishable by law if the victim is found guilty. In [6], the aim was to frame the user, however, in this work, the aim is to cleverly modify (tamper with) a file for personal gain. Johnston and Elyan [7] also discussed video evidence tampering; how the level of sophistication employed in this kind of attack has made differentiating the original video from the one tampered with more difficult.

Hardware-based attacks such as HID attacks are on the rise because more focus has been placed on countering software attacks due to their higher occurrence rate and this has caused a deficiency in protecting against hardware attacks [8]. Bojovic et al. [8] mention some of the advantages of hardware-based attacks which could make them a more attractive approach for attackers such as stealth because they are able to operate without relying on computer resources, they are undetectable by most antivirus programs, and they are usually platform independent. Hardware attacks often require some level of inside information or a man on the inside to be successfully executed as physical access to the target machine is often required. This makes attacks like this more effective because they are launched from within the organisation and as indicated by [9], attacks from within are more dangerous than those that originate from outside. Moreover, a lack of awareness on the methods and tools used to carry out some of these hardware-based attacks could lead a forensic analyst to a biased investigation in cases where the evidence might implicate an innocent party. As seen in [6], there is potential for the analyst

to take the evidence at face value and keep looking for more evidence to prove the guilt of the suspect. This form of bias could have several impacts on an investigation, resulting in an inaccurate conclusion by the analyst [10], and ultimately, a miscarriage of justice.

III. Experimental Setup

Fig. 1 shows the high-level experimental setup. The O.MG Cable has been configured to run in Access point mode which enables the attacker to connect to it wirelessly and control it from a distance. Two MS Excel records have been created; January_Contributions.xlsx and Comp2421_grades.xlsx. Both files are stored and managed on a local computer running Windows 10 which is the target computer for the attack (see Fig. 1). For the purpose of this experiment, someone is employed to manage these records and the employee is the user of the target machine. This person has the username 'Exp2_OMG_A' on the target machine. They are also responsible for the files on the target machine and any modifications made to them.

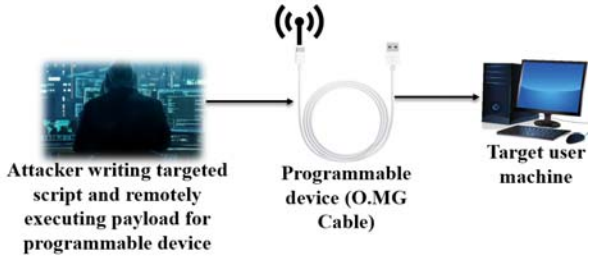

Fig. 1 Experimental setup

The target file is January_Contributions.xlsx which is a record of accounts paid where each user has a unique ID with other attributes (see Fig. 2). To make any changes to these files, physical access to the target machine where they are stored is required, along with knowledge of the file location and knowledge of the Windows Operating system, including the use of MS Excel and the unique ID of the target record. This experiment assumes this degree of knowledge. The attacker is interested in Mary Gold's record who has a unique UserID of '82589' (see Fig. 3). They want to alter the record to reflect a smaller amount for Mary's payment due, and also to change the payment status to 'paid'.

	A	B	C	D	E	F	G	H
1	UserID	FirstName	LastName	Department	Amount Due	Interest (%)	Payment Status	Next Payment Due
2	45621	Blessing	John	IT	3600	2.2	Paid	Feb-21
3	56789	Nancy	Love	HR	4200	2.2	Paid	Feb-21
4	98576	Maleek	Berry	IT	2650	2.2	Paid	Feb-21
5	24798	Jonathan	Stone	Compliance	[illegible]	2.2	Not paid	Feb-21
6	23987	Roy	Timberlan	HR	7500	2.2	Not paid	Feb-21
7	64658	Joshua M	Bliss	Compliance	3200	2.2	Paid	Feb-21
8	82589	Mary	Gold	IT	9500	2.2	Not paid	Feb-21
9	23145	Bidemi	Adenike	Compliance	3000	2.2	Paid	Feb-21
10	78982	Arnold	ksesprosky	Admin	4600	2.2	Paid	Feb-21
11	56874	Donna	Harvey	Compliance	5200	2.2	Paid	Feb-21

Fig. 2 Screenshot of January_Contributions.xlsx before modification

This attack also takes advantage of the unique ID attribute which is a property that uniquely identifies or distinguishes entities in a database or spreadsheet [11]. Using the unique ID, the attacker is able to specifically target and alter only the record of interest as opposed to using a name which may not be unique to one database user. Unique IDs are a key component of many databases and spreadsheets; however, with programmable devices like the O.MG Cable, and in scenarios like this where a particular record is targeted for tampering, the unique ID may be a vulnerability which facilitates the attack when it is known to the attacker.

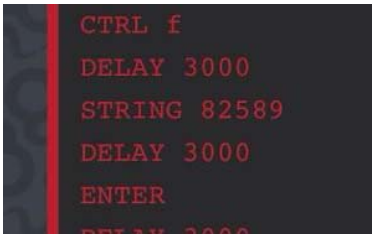

Fig. 3 Payload segment specifying the record of interest (82589)

This work highlights two possible scenarios where the attack being simulated here might be feasible:

1) A scenario where the O.MG Cable is plugged in while the employee is still seated at their computer, and the attacker pretends to want to charge their phone. The user of the machine is not suspicious of anything at all as the system did not make any sound or did not show any indications of something being plugged into it. The attacker requires only a minute to load and execute the payload already stored on the O.MG Cable from their mobile phone (or any device with a browser and wireless connection) from a few metres away. The fact that the O.MG Cable can be controlled remotely makes for a stealthier approach which would not arouse concern from the user of the computer because the O.MG Cable looks like a regular USB charger or data cable. As far as the employee is concerned, there is no one sat at their desk operating their computer and nothing 'untrusted' is plugged in; not even the silent, innocent looking USB charger without any device plugged to its other end.
2) Another potential scenario could be that the user borrows the attacker's charger, and on one occasion, the attacker takes advantage of this user's habit of borrowing their charger, to perform the file tampering attack. The user being sat at their machine while the cable is plugged calls for even less suspicion because the cable lies dormant and makes no sound or sign of connection until the payload is triggered by the attacker from the remote-control device (discussed further in the experiment results section). The cable could be plugged in to the machine for hours until the attacker finds a suitable window of opportunity when the user steps away and they would then remotely trigger the payload. As far as the user is concerned, no one was at their machine which indicates to them no one could have tampered with the computer or the files on the computer.

IV. Tools and Technology

O.MG Cable: This is the programmable USB being used here and it is the hacking device. The payload has been written, tested and stored on the O.MG Cable so it is easily loaded by the attacker from the remote device. Having the payload stored on the O.MG Cable helps save time, and ensure it is the tested version of the script that is being executed. This minimises the chances of typos or errors while typing the script afresh.

Mobile device: Having a mobile device such as a smart phone to control the O.MG Cable makes it less suspicious. An iPhone 7 was used for this experiment. The iPhone was connected to the O.MG Cable's wireless network and used to remotely load the payload to execute on the target machine. The iPhone served as the remote control for the O.MG Cable in this experiment.

Target machine: This is the Windows 10 computer containing the file of interest and it is on this same computer that the O.MG Cable is plugged in.

MS Excel: Microsoft Excel is a spreadsheet program for organising and managing data. The file of interest here is an excel spreadsheet stored and managed on the target machine. The O.MG Cable would need to use this program to modify the file of interest as though it were the actual user of the machine. MS Excel is part of the MS Office suite.

V. Implementation

The O.MG Cable was plugged in to the target machine and left for two hours before executing the payload. The assumption is that the O.MG Cable was plugged in while the employee was seated at the machine. After 2 hours when the employee steps away from the target machine, the attacker triggers the payload remotely from the mobile device. The O.MG Cable was left on the target machine up to one hour after the attack was carried out before it was unplugged. This simulates a scenario where the attacker may not get the opportunity to unplug the O.MG Cable immediately after executing the payload. The other file, Comp2421_Grades.xlsx had been modified by the employee two days before the attack.

VI. Experiment Results

This section examines the observations and findings during the operation of the programmable USB and during the forensic investigation. Autopsy 4.14.0 was used for the digital forensic investigation here.

A. Operational Observations

When the O.MG Cable is plugged in to the machine, it seems like the system does not detect anything being plugged as no sound of a connected device is heard from the computer. However, when the 'run payload' button is pressed on the remote-control device, the computer then makes the sound of a device being connected indicating that it now detects a device being attached to its USB port. Once the payload execution is complete, the computer makes a sound of device disconnection which would indicate that the O.MG Cable auto ejects itself once it completes execution of payload and becomes passive again. Further investigating the properties of the O.MG Cable, one of its capabilities includes "SURPRISEREMOVALOK".

If the O.MG Cable is not physically removed, it can still take a new set of instructions and reconnect to the target machine anytime a new payload is executed. It then disconnects itself again from the machine and becomes passive; appearing harmless but still with mobile charging and data transfer capabilities when a mobile device is connected to its other end.

B. Traces of the O.MG Cable on the Target Machine

The O.MG registers on the connected machine as three separate USBs in the registry. There was an instance of a device with a hardware ID of "VID_D3C0&PID_D34D, and two other instances with hardware IDs of "VID_D3C0&PID_D34D&MI_00" and "VID_D3C0&PID_D34D&MI_01". This was noticed and further investigated manually on a separate machine. It was discovered that the single device being split to two USBs represents a keyboard and a mouse. The hardware instance with the ID of "VID_D3C0&PID_D34D&MI_00" represents the mouse, and the other instance with an ID of "VID_D3C0&PID_D34D&MI_01" represents the keyboard functionality of the O.MG Cable.

There was no device make (i.e., manufacturer) found for the O.MG Cable while investigating attached USB devices. A unique device make might make it easier to spot the programmable device and know it is one of the malicious ones. The trusted and recognised USB devices have their device make present. The O.MG Cable, apart from being installed as two separate devices, also has an installation instance as a single device with a weird 3-digit device ID of 999. This device ID, when compared to the other device IDs present should raise suspicions. Device IDs for the mouse and keyboard instance are 6&280dd913&0&0000 and 6&280dd913&0&0001 respectively. The three installation instances have identical time stamps.

C. Traces of the O.MG Cable on the Target File

Fig. 4 shows the metadata of the January_Contributions.xlsx file, and as can be seen, the last author of the file shows "Exp2_OMG_A" which is the username of the logged-on user. Again, this is expected because a malware operates within the security context of the current or active user; therefore, the O.MG Cable assuming the username of the active user is not surprising. Installation time of the O.MG Cable was 2021-08-09 16:37:12BST and the modified time of the file shows "2021-08-09 16:38:53BST" which is about 2 minutes after the installation of the O.MG cable.

The timeline of actions (device installation and file modification time) seems close here because the O.MG Cable in this case has been programmed to carry out the instructions without too much delay. Therefore, the timeline of actions may not be the best to rely on here as this could be a coincidence of timing where the O.MG Cable was programmed to perform a totally different set of actions. The timeline of actions may not also be the best to rely on because the O.MG Cable can be programmed with a delay before execution and delays in-between execution of instructions. The file properties of the

January_Contribution.xlsx and Comp2421_grades.xlsx are similar. The file sizes, hashes, and last modified time however are different but this is expected because their contents are not the same and they were not modified at the same time. The main point here though is that there is nothing on the target file to raise the forensic analyst's suspicion; neither are there any notable differences between the file altered by the computer user, and the one altered by the O.MG Cable. Table I summarises the outcome of the experiment and it shows the employee as the person responsible for last modifying both files.

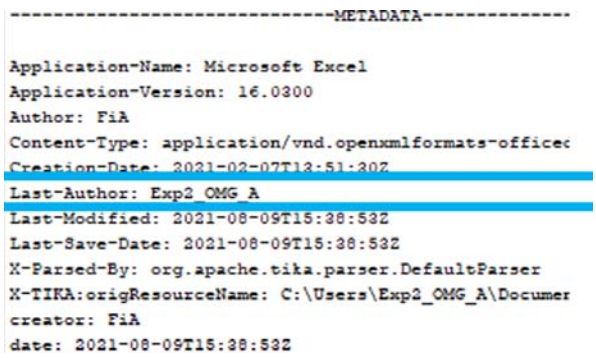

Fig. 4 Target file metadata after unauthorised modification

TABLE I
SUMMARY OF RESULTS

File name	Comp2421_grades. xlsx	January_Contributions. xlsx
File type	MS Excel (.xlsx)	MS Excel (.xlsx)
File last altered by	Employee	O.MG Cable
Meta-data last modified by	Exp2_OMG_A	Exp2_OMG_A
Any flag by the forensic tool?	No	No
Any unusual file properties?	No	No

More in-depth analysis is required; however, *prima facie* this experiment shows that the device is capable of perfectly modifying records and files without the forensic tools being able to differentiate between files modified by the user and files modified by the O.MG Cable. There are traces on the target machine to indicate the presence of an attached USB which has been identified to be the O.MG Cable. However, there are no direct links between this attached USB to the actions carried out on the file. This in turns leads to the question whether investigators would even consider the presence of some unidentified USB as responsible for modifying a file? The most likely answer would be a 'no' because the limited knowledge in this area means investigators, are less likely to be aware of the availability and usage of devices like the O.MG Cable. If the user were also asked if they saw anything suspicious being plugged, their answer would not include the O.MG Cable because as far as they are concerned, it was only a phone charger, and no phone was even plugged to its other end. The user could also be asked if someone else had used their computer that day, and their answer would also most likely be a 'no' whereas in fact, someone did; not just in person but through a cable.

VII. EVALUATION

Since the O.MG Cable also modified the file while a user session was active, its operations assume the credentials of the logged-on user. That is, it operates within the context of the current user so most activities performed by this device would carry the name of the user making it appear like the user is responsible for whatever actions were performed including file creation or file modification which is the scenario considered in this work. According to [3], this can be considered a form of identity theft.

The speed of execution of this programmable device is one of its strengths as it can carry out tasks very swiftly; however, its speed could also be its shortcoming like the Rubber Ducky [6]. Both programmable devices execute instructions line by line, therefore, if as little as just one line of the payload is executed at the wrong time, the entire order of execution could be affected. The speed of the target computer could also influence the success or failure of this kind of attack. For example, if the payload script was written to execute with very little or no delays, this might be too fast for the target computer to keep up with carrying out the instructions. The O.MG Cable by default would not wait to check if the last instruction has been carried out or not before executing the next, so they continue with the payload execution until all lines are executed at the programmed time; even though the target machine may still be busy or hung up on the third line of instruction out of twenty lines (just for example). The O.MG Cable has two advantages over the Rubber Ducky in this regard: firstly, instructions can be sent remotely with the O.MG Cable. Secondly, payloads can be modified on the fly (i.e., without disconnecting or unplugging) with the O.MG Cable which is not the case with the Rubber Ducky. The attacker would need to gain physical access to the Rubber Ducky and unplug it to modify the script, re-encode the script, reload the encoded payload onto the Rubber Ducky, and then physically re-plug or re-attach on the target device. Depending on the scenario or the kind of attack to be performed, this might not be feasible without getting caught or suspected.

VIII. CONCLUSION

Following this experiment, the O.MG Cable could be considered one of the most dangerous programmable USBs available because of its camouflage and dual feature as a mobile device charger/data cable. Most people have a mobile device, and these devices need a charger, making it easy to carry the O.MG Cable almost anywhere, and plug into any available port without raising suspicion. Apart from the O.MG Cable's ability to modify files like a human user, it could also be used to perform other unauthorised or illegal actions on the target machine, making it appear like the user of the machine is responsible for the actions carried out. The chances of suspecting a simple cable as responsible for these actions are very slim, especially if forensic tools or analysts are also not able to pick this up easily, not aware of the capabilities of these programmable devices, or not aware of these programmable devices at all.

As discussed earlier in the literature review, the lack of awareness of the availability and impact of tools like the O.MG Cable could also lead to bias in an investigation, where the forensic analyst takes the evidence at face value. Bias could impact an investigation in a number of ways, which could lead to errors in the forensic result [10]. The forensic analyst might keep looking for more evidence in the direction of implicating the suspect without considering other possibilities and may also draw their conclusions to show the suspect is guilty based on the same evidence they have taken at face value. An even bigger problem with this is that the analyst's conclusion, though biased in this case, could still be perceived to be credible. This could lead to inaccurate expert testimony in court, ultimately leading to a miscarriage of justice where an innocent person is prosecuted for a crime they did not commit. The first step towards an unbiased analysis in this kind of situation, is to be aware of all possible subjects that could be responsible for the actions on the object(s) in question. In this case, analysts should be aware that there are programmable devices with the capability to carry out actions like a human user would, including creation or modification of files. There is therefore a need to have a viable and reliable methodology to investigate the presence or actions of programmable devices in difference scenarios where their use is a possibility. This will help increase the confidence in forensic results in cases where a programmable USB might have been used; by so doing, mitigating the chances of a wrong conclusion by the analyst, mitigating the chances of an inaccurate testimony, and ultimately mitigating the likelihood of a miscarriage of justice.

In this work, an assumption of prior reconnaissance was made; however, future work would involve reconnaissance using another portable programmable device such as the Screen Crab to gather information and monitor the user's activities in order to more efficiently plan and execute the file tampering attack. Future work will also involve testing with other programmable devices in different and more complex scenarios to investigate the presence and potency of programmable devices, and to ensure their actions can be reliably distinguished from the actions of a human user. This will help increase the level of assurance in forensic results where the use of a programmable device is a possibility.

REFERENCES

[1] Kumar, Y., 2020. Juice Jacking-The USB Charger Scam. Available at SSRN 3580209.

[2] Grobler, C.P., Louwrens, C.P. and von Solms, S.H., (2010). 2010. A multi-component view of digital forensics. In 2010 International Conference on Availability, Reliability and Security (pp. 647-652). IEEE

[3] Dean, P.C., Dean, P.M. and Dean, J.L., 2016. Identity theft: What you don't know could hurt you. International Journal of Business and Social Science, 7(8), pp.1-4.

[4] Loe, E.L., Hsiao, H.C., Kim, T.H.J., Lee, S.C. and Cheng, S.M., 2016, December. SandUSB: An installation-free sandbox for USB peripherals. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 621-626). IEEE.

[5] Kitchen, D., (2016). 2016. hak5darren/USB-Rubber-Ducky. (online) GitHub. Available at: https://github.com/hak5darren/USB-Rubber-Ducky (Accessed 29 Feb 2021).

[6] Lawal, D., Gresty, D., Gan, D., and Hewitt, L., 2021. Have You Been Framed and Can You Prove it? In 2021 44th International Convention on Information and Communication Technology, Information System Security (MIPRO). IEEE.

[7] Johnston, P. and Elyan, E. (2019). 2019. A review of digital video tampering: From simple editing to full synthesis. Elsevier, (online) 29. Available at: https://www.sciencedirect.com/science/article/pii/S1742287618304146 (Accessed 13 Nov. 2019).

[8] Bojovic, P.D., Basicevic, I., Pilipovic, M., Bojovic, Z. and Bojovic, M., (2019) 2019. The rising threat of hardware attacks: USB keyboard attack case study. Journal of IEEE Security & Privacy.

[9] Sanzgiri, A. and Dasgupta, D., (2016). 2016. Classification of insider threat detection techniques. In Proceedings of the 11th annual cyber and information security research conference (pp. 1-4).

[10] Sunde, N. and Dror, I.E., (2019). 2019. Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital Investigation, 29, pp.101-108.

[11] Wigmore, I., 2019. What is a UID (Unique Identifier)?. (online) IoT Agenda. Available at: https://internetofthingsagenda.techtarget.com/definition/unique-identifier-UID (Accessed 12 October 2021).