Air Hopper Malware

G V S N Sobhan
Computer Science Engineering, Kalasalingam University, Madurai India
sobhansai45@gmail.com

Sanjay Ragavendra.R
Computer Science Engineering, Kalasalingam University, Madurai India
sanjayvay@gmail.com

Abstract— This is basically a proof of concept malware that is used in stealing data from isolated computers. This is used to access data in computers which have no internet access hence making it difficult to compromise. Radio signals are transmitted and makes it possible to extract the data using mobile phones and various other sources. Numerous organizations have sorted to "air gapping" that keep information safe and this method allows us to overcome that security measure. This mechanism is efficient enough to steal a security password which by means is more than enough to get what the hacker needs.

We make sure we adapt the communication system to implement a stealthy communication by using different high range frequencies. Various forms of key logging over multiple hops are presented. This is also a network stack that was designed for communication in robust places. There are various applications that are implemented and used for these methodologies. There are also various counter measures for air hopping such as systems that have intrusion detection systems that allow to detect any irregularities and finally this method is not all that effective due to extremely sophisticated security systems.

Keywords- Air Gapping, Air hopper, GSMem, TELMAT, malware, wireless communication..

I. INTRODUCTION

Air gap is generally a malware which is used to detect or defeat the air gap solution in securing the computers which are using the various air-gap convert channels. The most sensitive data are usually "air gapped" isolated from the internet. There's no need to connect to other systems that are internet connected and their Bluetooth feature is disabled also.

The malware can be attacked on the computers in various ways, including the removable disks and other various software and hardware components. In this process the difficult process is making the malware to give the sensitive data from the affected pc.

Many researchers have said that the unauthorized accessing or copying of the data from a normal computer can be done through the radio signals captured by a mobile device. The "Air Hopper" concept uses the computers graphic card to emit electromagnetic signals to a mobile device for capturing the data.

The attacker can attack a computer in mainly four steps. They are

1. Introducing a piece of malware into the computer.
2. Mobile code installation on mobile phones.
3. Attacker sets a command and control (C&C) channel with the mobile phone.
4. Transmitting signals from the computer back to the attacker.

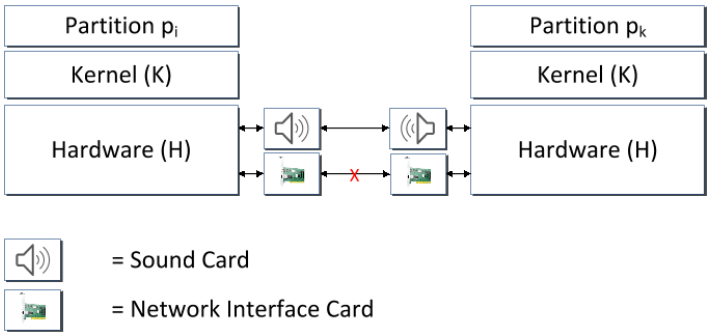
The malware is first introduced into the computer which means the information that the hacker requires is already on the way. The next step after establishing this is to gain access to it using a mobile phone. Here to attacker has a medium of access. This is the establishing mechanism of the Air Hopper. Once a connection is established then data transfer is bidirectional. This is how it works.

The malware installed in mobile uses the receiver of FM radio to receive the signals, which have been modulated with information sent by the malware on computer with the use of the cable attached to the monitor. Once it has been transferred then the data is transferred to the attackers mobile phone via internet or through a message. In some of the organization they will bring their own device which will be an easy way for the attacker to infect the malware.

We use Rootkit placed in the baseband firmware of a nearby cellular phone.. We get crucial data such as

- Signal generation
- Data modulation
- Transmission and detection

Effective transmission is possible over a distance of 30mts.



Security Malware Acoustic Mesh Network:

With the protected channel we can overcome system and network security policies by exploiting new and unregistered communication forms. In operating systems the level of communication is very covertive, but if the inner channel of communication is accessed in the operating system then all the resources can be shared.

Once these resources are accessed then the network interfaces among all the connected computing systems can be accessed. So, by emanating different radio frequencies we can gain access to not only one system but all the connected systems efficiently. Generally existing radio communication standards are more than enough for our scenario.

- It can be used for sending and receiving.
- It has an input or output of physical emanation type.
- It supports stealthy communication.
- Hence it is not subject to the system and network policies.
- The information is fully accessible to the sending or receiving process.

In the above instructions we specifically target stealthy communication networks over acoustical emanations that are of the physical type which utilize the sound systems of a device as they are the first parts of a computer system that are capable of receiving radio frequencies. Look at Step 1 we mention that it can send and receive, hence its bidirectional. Also it covers both in the form of input and output. Further since it's a stealthy network the communication is covert. As of Step 4 since the speakers or microphones do not get covered under any network or security policies, it is very easy to exploit them. There is an acoustic wave process that has been found in order to access the operating system via propagations which will be further addressed.

We do not specifically address communication between two computer systems. This involves accessing two isolated application in a system, the disk partitions and further on.

The major use of security mesh network system is underwater. More than looking at it as a form of an attack look what it can do. Now that we are sure that telecommunication is not possible underwater or as we can say not reliable, we have to depend on other means such as this. Which ensures that the messages that has to be passed on is done so properly. Further we feed this network with a multi hop form of communication so it is more enhanced and capable for longer distances of communication.

So one a whole we take section one where we introduce the concept of the mesh networks and the forms of communication possible with them.

And also in section two we present the fundamental concepts of the mesh networks.

There is an experimental setup for this concept that has been performed and corrected on the acoustical mesh network.

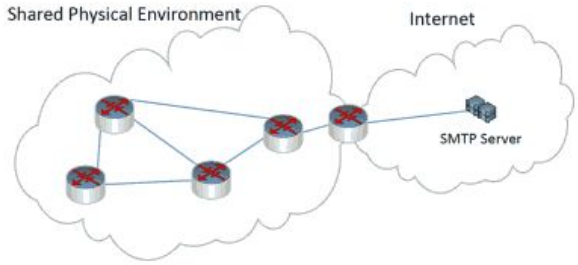
There are various applications that are used in these networks and are presented.

As of the conclusion of this article we look at a future perspective of this concept. Ever since the concept of acoustical mesh networks have been introduced there are huge improvisations to it and also counter measures to efficiently tackle all the incoming transmissions.

There are three types of participants in a secured mesh network.

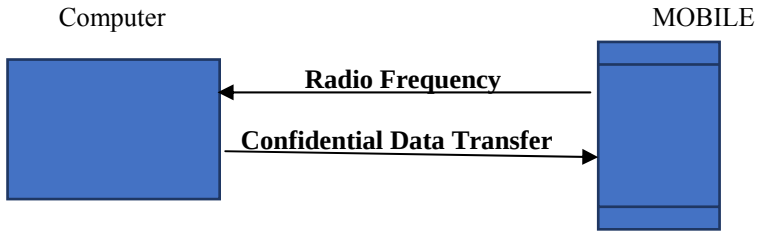
There is the Attacker, infected victim and the infected drone.

There are finally the computing system controlling the covert mesh and the receiver of leaked information



Topology of an acoustic security malware mesh net

II. OPERATION AND MECHANISM



Data Transfer from a normal organisation computer to mobile phone of attacker.

The main concept in the field of research about air gapping is to use RF in order to transmit the confidential data from the computer to the mobile phone. Air hopper explains how textual and binary data can be extracted from a normal physical device to mobile phones.

In modern world in which most of the people using the laptops which have a built in microphones and speakers, this malware is used for communicating information acoustically secure, at a range of frequencies beyond the normal human hearing limit. This technique is limited to the computers which are physically close and also which can be used for short distance transmitting and receiving information through a malware link.

This transmission can be overcome by using a mesh network which can be acoustically linked, which will be more effective with a Ethernet connection to the outside world through which secure information can be removed using secure facility.

This transmission from a computer to a mobile phone on a distance of up to 23 feet at 13-60 Bytes per second, which researchers say is enough to steal a secret password

Vulnerabilities of a radio channel:

The bitter experience in the career of NSA, which has been secretly using a same pattern of siphon for six years. The spy tools catalogue of the NSA has been leaked online last year describing that the radio frequency signals used by the computer remotely siphon the data using transceivers which are attached to or embedded within the system. But the exact technique used for this loss has been never revealed.

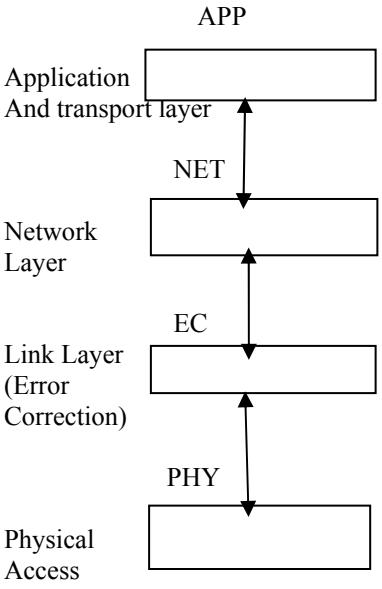
The Air Hopper by the researchers which allows the hackers and spies to secretly siphon passwords and the other data from the computer. This attack borrows the radio signals which can be generated by a computer video card. The researchers in Israel have created a malware which will overcome this vulnerability of the radio frequency signals which can be generated and can transmit the data which is received is the decoded by the FM radio receiver in mobile phones. These receivers can be used an emergency backup, for receiving the radio transmissions when the network is not available. Though the organizations or companies think that they are protected in the environment detaching them from the world but there is a possibility of being attacked through the mobile phones of the employees which will be giving the attacker an easy way to reach the confidential data.

COMPOSITION OF THE UNDERLYING COMMUNICTION SYSTEM:

Network Stack:

It is the general form through which electromagnetic waves are sent under water. The bunch of components which are used are split into four layers of connected applications.

- Application layer
- Error Correction layer
- Physical link layer
- Network layer.



Application Layer:

This is the layer where all the applications that were meant to be used for acoustical mesh networks. Here the processed frames are sent to the network layer via a tcp connection.

Network Layer:

In the network layer we receive the frames which are used and further processed for output.

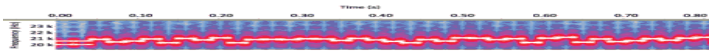
Eg: GUWAL, GUWManet.

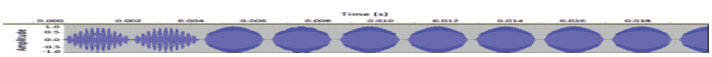
The GUWAL network is mainly used for network routing. GUWManet is used for header changes.

Link Layer:

Error Correction layer:

Both the sender and the receiver can benefit from optional error correction. The layer uses a 16 it checksum.





Signal waveform—the preamble and 6 transmitted bits are made visible

III. LIMITATIONS

Air hopper a bifurcated attacked pattern showed us how to extract confidential data to transfer to a nearby mobile phone using FM frequency signals.

Bit Whisper:

The data can be extracted bidirectional from mobile phone to computer and vice versa using thermal manipulation mechanism which doesn't include any extra peripheral devices.

GSMem:

In this particular mechanism we used cellular frequencies to gain access to air gapped systems. This includes transmission generated by a standard internal bus.

Project Sauron:

This is a malware that uses a USB which is infected and can be used to remotely leak data of a computer. Overall in general it can be claimed that various hardware mechanisms can be used to leak sensitive information from air gapped systems using what is known channels.

Mediums with which an Air Gapped system can be accessed:

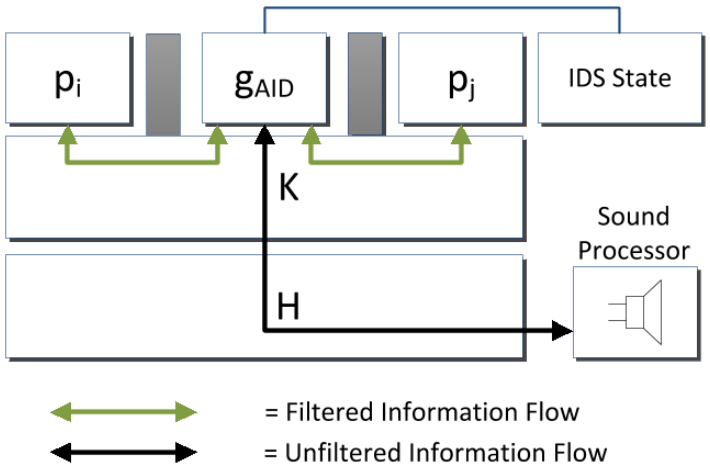
- Acoustic
- Light

Counter Measures:

Working with Audio Filtering Options:

Suppose we have a system that cannot be switched off these audio filtering options are very useful.

There is also a host based audio system that acts as an operating system guard. Hence peripherals like speakers or microphones cannot be accessed.



IV. APPLICATIONS OF MESH NETWORKS

Key Logger:

The infected victim sends all recorded key strokes that are accessed easily by the attacker hence there is a loss of valuable information. The key logger is configured to write any key strokes.

Tunneling:

There are various complications in intermediate networks with which the gap can be closed via the tunneling process.

V. ADVANTAGES

It is used in the military, government and financial systems.

There are various classes of people and organizations that use this mechanism.

All these set of groups carry sensitive information. Air gap can also be used as a stable environment for sensitive application development.

It can be used to have a controlled mechanism for systems that are self-contained and do not need any external sources of control.

Nuclear equipment, engine control and various other methods of controlling data in a safe manner is based on Air Gapping.

A Malware installed on a compromised machine can generate acoustic emissions at specific audio frequencies by controlling the movements of the hdd-s actuator Arm. Digital information can be modulated over the signals and can be picked up by a nearby receiver.

Based on our method we develop a transmitter on a personal computer and a receiver on a smart phone and we provide the design and implementation detail.

There is an application called Disk Filtration. With this process, we are able to transmit data from Air gap computer at an effective bit rate.

The mesh system is not widely used on normal grounds. I t is based on underwater communication.

Software Defined Parameter

It is a framework which is referred as virtual air gapping and it requires authentication from external end points who are trying to access internal facilities which ensures that only authenticated systems can see internal IP address.

VI. CONCLUSION

We come to a conclusion that the air gapping system is not really as protective as people think it is, the mechanism to overcome an air gapped system is to use a malware called Air Hopper. After Air Hopper, various types of methods have been introduced in order to extract data from an isolate system. There are various medium in which the data is accessed. We further have analyzed how the data can be prevented from being accessed. There a theory on however secured an air gapped system can be there will always be means with which we can access the files. Stealing one small aspect of the system or even a small security password is enough to put the air gapped system into trouble. After the introduction of meh networks we also understood that air hopper isn't the only mechanism that is used. We have other sources via which information can be accessed. There are several applications that can make it easier to do. We looked at how electromagnetic waves play an important role. The mesh networks are mainly used in underwater transmission. The paper concludes saying that as the measures of keep data safe improves there are constant counter actions for this. We also saw all the advantages and the drawbacks of the mesh as well as the hopper system. In some cases of highly protected system sometimes these measures fire back. Information cannot be extracted as well as it is required to. So the softer parts of a system are targeted.

ACKNOWLEDGMENT

We take immense pleasure in thanking Muthamil Sudar.K who guided upon choosing our topic and we further thank Mrs.A.Nesarani who taught us the networking aspect of Air Hopper Malware

REFERENCES

[1] Carrara,Brent, Linear Networks and Systems (Book)
[2] Michael Hanspach "Acoustical Mesh Networks in Air"
[3] S.Sibi Kumar, "Air Hopper Malware"(unpublished), wikipedia.com
[4] Moderchai Guri "How to leak sensitive data from an isolates system, "to be published.
[5] E. Blossom, ―GNU radio: Tools for exploring the radio frequency spectrum,‖ Linux J., vol. 2004, no. 122, June 2004.
[6] T. Halevi and N. Saxena, ―A closer look at keyboard acoustic emanations: Random passwords, typing styles and decoding techniques,‖ in Proc. 7th ACM Symposium on Information, Computer and Communications Security, New York, USA: ACM, 2012, pp. 89–90.
[7] D. Balzarotti, M. Cova, and G. Vigna, ―Clear Shot: Eavesdropping on keyboard input from video,‖ IEEE Symposium on Security and Privacy, pp. 170–183, 2008.