Transfer of Malware and Prevention Technique via Ultrasonic

M. Kailesh, J. Godwin Ponsam
Dept. of Information Security and Cyber Forensics
SRM University, Chennai

Abstract – **Existing covert channel communication used to circumvent system and network policies by establishing communications that have not been considered in the design of the computing system. A new system to construct a covert channel between different computing systems that utilizes audio modulation/demodulation process to exchange data between the computing system to implement covert and stealthy communication by producing ultrasonic frequency in the standard laptops using Software Defined Radio (SDR)as a platform with GNUradio with Embedding TCP protocol stack. An approach of using Malware (i.e.,) using Botnet via communication protocol as to perform attack over covert mesh networks as not yet accomplished in previous research. To attain data rate as greater than 20 bits/sec. At last, the countermeasures against covert acoustical mesh network are introduced using low pass filtering and host based audio intrusion detection system for analyzing audio input and output.**

Keywords – **Covert channel, Ultrasonic, Botnet, low pass passive filter.**

I. INTRODUCTION

Covert channels are communication channels utilizing means for communications that have not been designed for communication at all. With a covert channel, we can circumvent system and networksecurity policies by exploiting new, previously unregardedcommunication media. In operating systems, covert channelsare usually established by exploiting shared resource accessbetween different processes, establishing a covert storagechannel by encoding data in parts of the operating system thatwere not considered for communication at all or establishinga covert timing channel by manipulating and analyzing thetiming behavior of shared resources. In computer networks,covert storage channels can be established by utilizing normallyunused parts of communication protocol headers andcovert timing channels could be established over the timingbehavior of network requests.

The term covert channel is so called because it is hidden from the access control mechanisms of ultra-high-assured secure operating systems since it does not use the legitimate data transfer mechanisms of the computer system such as read and write, and therefore cannot be detected or controlled by the hardware based security mechanisms that underlie ultra-high-assured secure operating systems. Covert channels are exceedingly hard to install in real systems and can often be detected by monitoring system performance: in addition, they suffer from a low signal-to-noise ratio and low data rates (on the order of a few bits per second). They can also be removed manually with a high degree of assurance from secure systems by well-established covert channel analysis strategies.

Covert channels are distinct from, and often confused with, legitimate channel exploitations that attack low-assured pseudo-secure systems using schemes such as steganography. The legitimate channel misuse by steganography is specifically not a form of covert channel.

Covert channels can be tunnel through secure operating systems which can be tunneled through recent operating systems and require special measures to control. Covert channel analysis is the only proven way to control covert channels. In contrast, secure operating systems can easily prevent misuse of legitimate channels. Distinguishing these is important. Analysis of legitimate channels for hidden objects is often misrepresented as the only successful countermeasure for legitimate channel misuse. Without being informed of this, some are misled to believe an analysis will "manage the risk" of these legitimate channels.

Ordinary things, such as existence of a file or time used for a computation, have been the medium through which a covert channel communicates. Covert channels are not easy to find because these media are so numerous and frequently used.

ISSN: 2278 – 1323

Two relatively old techniques remain the standards for locating potential covert channels. One works by analyzing the resources of a system and other works at the source-code level.

There is proof of concept of existence as well as exploitation of covert channels in TCP/IP protocol suite. This work can, thus, be regarded as a practical breakthrough in this specific area. The adopted encoding and decoding techniques are more pragmatic as compared to previously proposed work. These techniques are analyzed considering security mechanisms like firewall network address translation.

However, the non-detectability of these covert communication techniques is questionable. For instance, a case where sequence number field of TCP header is manipulated [7], the encoding scheme is adopted such that every time the same alphabet is covertly communicated, it is encoded with the same sequence number.

Moreover, the usages of sequence number field as well as the acknowledgment field cannot be made specific to the ASCII coding of English language alphabet as proposed, since both fields take into account the receipt of data bytes pertaining to specific network packet(s).

The Data Hiding in TCP/IP Protocol [4] suit by covert channels have following aspects:

1. Identify the existence of covert channels in a network environment.
2. Point to satisfying techniques of embedding and extraction processes at the source and destination.
3. Do not consider the effect of employing covert communications network as a whole.

II. OBJECTIVE

To construct a covert channel between different computing systems that utilizes audiomodulation/demodulation process to exchange data between the computing system to implement covert and stealthy communication by producing ultrasonic frequency range(above 20 kHz) in the standard laptops using Software Defined Radio(SDR)as a platform with GNUradio. An approach of using Malware(i.e.,) using Botnet via communication protocol as to perform attack over covert mesh networks as not yet accomplished in previous research with the GUWAL protocol [1]. To attain data rate as greater than 20 bits/sec. At last, the countermeasures against covert acoustical mesh network are introduced using low pass filtering and host based audio intrusion detection system for analyzing audio input and output.

III. SCOPE

The establishment of covert channel in air is feasible in setups with commonlyavailable business laptops. By utilizing low ultrasonic frequency using GNUradio a Software Defined Radio(SDR), we take advantage of a network stack thatwas built with robust USRP communication in mind. Thepresented approach to covert legitimate networks allows to transmit messages with a rate of approximately 30 bytes/s upto a range of around 10-15 m between two connected nodes [2], but muchhigher transmission rates would be possible for low-distancetransmissions.

IV. EXISTING SCENARIO

The implementation details of the utilized acousticcommunication system in previous approach using GUWAL protocol, (a Generic Underwater Application Language) [1] are described in a brief process below.

A. A Network Stack for Acoustic Communication

Acoustical communication is seldom seen in terrestrialnetworks since radio offers much higher bit rates and communicationranges. However, acoustical communication is themethod of choice in underwater networks, because electromagneticwaves are highly absorbed by sea water. We are,therefore, able to implement a terrestrial acoustical network ontop of preliminary studies about robust underwater acousticalcommunication.

The utilized network stack is an adaption of an emulationsystem for underwater acoustical networks from theResearch Department for Underwater Acoustics and MarineGeophysics (FWG) of the Bundeswehr Technical Center WTD71 in Kiel, Germany. It is split into four layers of connectedapplications (not to be confused with the TCP/IP stack):

1) Application Layer (APP)
2) Network Layer (NET)
3) Error Correction Layer (EC)
4) Physical Link Layer (PHY)

All layered applications of the network stack are independentand connected via internal TCP connections for IPC(inter-process communication). This structureallows to replace

ISSN: 2278 – 1323

any of the modules, e.g., the applicationlayer module, without the need to touch one of the other layers.The error correction layer is optional and can be left out ondevices with limited processing power or memory.

V. GNURADIO MECHANISM

GNU Radio is an open source toolkit for developing software radios. GNU Radio uses a combination of C++ and Python language. The computationally intensive processing blocks are implemented in C++ while application-defined control and coordination of these blocks are developed in Python. In particular, GNU Radio provides a signal processing runtime environment which, combined with (low-cost) external RF hardware, allows live SDR applications. Here we focus on the current version 3.7.5. Before detailing GNU Radio's working mechanism, we need to introduce some core software modules: GR block, GR buffer, flow graph, scheduler, and GR top block. A GR block encapsulates a computational phase which implements various data/signal processing functions, such as a filter, a decimator, or a modulator. Depending on the exact function, a block may have one or multiple data/signal input stream(s) and/or output stream(s). GR buffers are used to connect blocks together. A particular combination of connected blocks is a flow graph. GNU Radio applies its own schedulers for scheduling computation across blocks within a flow graph at runtime.

VI. PROPOSED SOLUTION

Using the covert channel communication to implement data transfer using GNUradio software for data transmission [9] by Botnet communication protocol to achieve the data transmission rate more than existing one.TCP as a network protocol layer to embed the GNUradio a SDR to create a covert channel by utilizing unused fields that are not used while legitimate transmission such as identification, fragment offset, header checksum, options in IPv4 for hiding data into that. This is also termed as steganograph.

GNUradio uses this fields into TCP/IP header [4][7] as a input stream for fragmenting data bit by bit and processed to each block of flow graph for transmitting as ultrasonic frequency.

Another target of increasing the data transmission rate.By transfer of botnet and analyzing their activities through ultrasonic waves, and an approach of using lowpass filtering and host based intrusion detection system to avoid such higher frequency transmission.Now a days attacks in covert channel is the emerging one so to prevent such intrusions as in one form of vulnerable way.

A solid proof has been undertaken from ultrasonic communications methods in air, using a quadrature modulation method. Simulations were first performed to establish the likely performance of quadrature phase shift keying over the limited bandwidth available in an ultrasonic system.

Quadrature phase shift keying modulation was then implemented within an experimental communication system, using capacitive ultrasonic sources and receivers [3].

The results show that such a system is feasible in principle for communications over distances of several meters, using frequencies in the 200 to 400 kHz range [3].

Though this system of implementing malware as in previous research has not addressed the problem of how to infect computing system through malware.

So to implement a Botnet communication protocol that includes

- Internet Relay Chat
- Hyper Text Transfer Protocol(HTTP)
- P2P

The overall setup process includes the below components which were used in GNUradio including covert channel creation, data transfer through covert channel, modulation and demodulation process.

1. FREQUENCY XLATING FIR FILTER

Implements a frequency-translating FIR filter. This is often used as a utility channel selection block, as it performs frequency translation, channel selection and decimation in one step.

2. RATIONAL RESAMPLER

Combined Interpolator and Decimator. This block is used to convert from one sample rate to another as long as they can be related by a ratio: Fs_out = Fs_in x Interpolation / Decimation. Note that all blocks following this block in the flowgraph should expect the output sample rate.

ISSN: 2278 – 1323

3.GFSK MODULATION AND DEMODULATION

Gaussian Frequency Shift Keying is a subclass of CPFSK (Continuous-Phase Frequency Shift Keying) and is related to MSK (Minimum Shift Keying). Stated shortly GFSK modulation is Gaussian low-pass filtered binary pulses, resulting in smooth or rounded pulses, which are then frequency modulated. As far as comparing with GMSK modulation, quantifying the signal processing complexity in SDR is critical to ensuring that the system has sufficient computational resources to support reliable digital communications [5]. Thus GFSK may be viewed as more similar to the analog modulation FM, GMSK than to FSK, this is also evident in the demodulation procedure.

In addition to the property of a continuous phase, like CPFSK, a GFSK modulated signal is also smooth at all times, and thus exhibits no discontinuities in neither the phase nor frequency. This ensures a limited spectral bandwidth of the GFSK modulated signal.

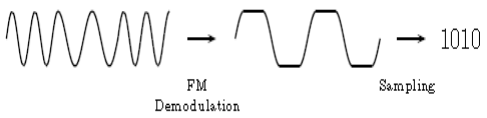


Fig. A1 GFSK Demodulation

The FSK signals cannot be demodulated directly, and have to be demodulated indirectly. Indirect FSK demodulation consists of two parts; frequency demodulation and a decision part, this is illustrated in Figure A1. Indirect demodulation results in a signal where the change in frequency is expressed as change in amplitude, effectively transforming the signal to an amplitude modulated signal. For the decision part the simplest approach is a threshold determining whether the transmitted symbol corresponds to a binary zero or a binary one. The decision part of the demodulation process is primarily interested in relating to analog network coding. For frequency demodulation the simple and cheap method is called Phase-Shift Discrimination is used.

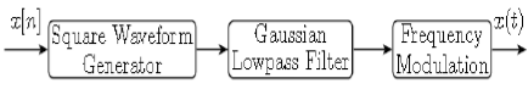


Fig. A2 GFSK Modulation

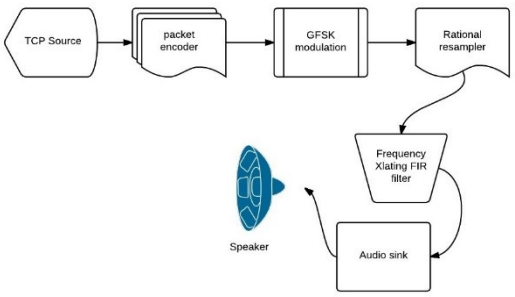
Modulation of a Gaussian Frequency Shift Keying signal is performed in three steps, first a square waveform is created from the binary signal (x[n]), represent the square waveform is passed through a Gaussian low-pass filter, and last the generated baseband signal is frequency modulated i.e. changes in amplitude is expressed as change in frequency. This is illustrated in Figure A2.

4. WX GUI FFT SINK

When the USRP source goes to a WX GUI FFT sink and WX GUI Scope sink. They appear to be a good tools for sanity checks. One feature that should needs to examine a portion of FFT spectrum more closely. Here an option it can specify the start and stop frequency for the FFT spectrum display for accurate output result.

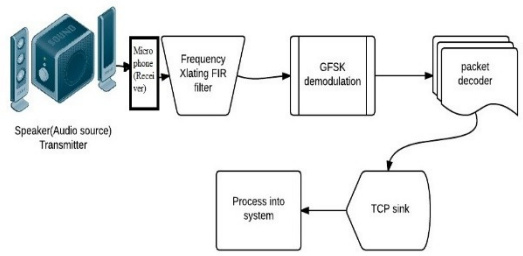
VII. EXPERIMENTAL SETUP

The developed model for transmission of data using covert channel communication is by including the above components in the SDR of GNUradio [9]. As per the thesis done for SDR with wireless protocols [6] helps more for accomplishing such model. This possible approach can be done by first injecting the legally usable SDR into target system by the process of virus program or through a normal Trojan dropper. Here the proposed and implemented model is only developed for the phase of transmission of infected data bit by bit to the target system and to collect the infected data bit by bit to a pool of data in organized manner. This developed model will do that of all the process explained in this paper. The architecture of developed model is described in a diagrammatic scenario 1.1 and scenario 1.2.



Scenario 1.1

ISSN: 2278 – 1323



Scenario 1.2

With the sample rate of 48kHz and TCP source as combined with malware bytes as data which is transmitted from TCP source through packet encoder for invisible content i.e., legal packets are assumed by operating system and allows transmitting to the target system. Meanwhile in Frequency Xlating FIR filter comprises of center frequency of 23k frequency for translation after the process of modulation from GFSK modulation with BT of 350m. These frequency finally undergone into audio sink to produce as audio waves with invisible content of malware bytes from Source. This will received by a microphone of the target system which is already linked with the port number accepted by both source and destination machine for covert channel communication. As similar to transmission the components are vice versa in reverse processing of components which have done with transmission for demodulating the signal and the carrier wave, with the malware bytes binded within the transmitted frequency. This is possible by using low passive frequency that our laptops or desktops neither check nor filter these frequencies, ultimately this becomes the vulnerability in system software as well as in hardware too.

This experimental scenario is made up with three standard laptops of minimum configuration of basic requirements but in the absence of wireless communication i.e., such as Bluetooth, Wi-Fi, Infrared, NFC [8]. This utilizes only the sound waves emitting from the normal in build speaker and microphone of our laptops. The frequency range of 48 kHz i.e., under ultrasonic frequency range of communication happens here with this development model. Bit by bit transferring assumes that a 20 MB size of data is transmitted or received in a month of period.

VIII. CONCLUSION

The GFSK modulator is better for Ultrasonic frequency communication in air. In SDR the wireless protocols were reliable of transferring data more of FSK, GMSK, FM, with a full-fledged GFSK is used. The need of transfer speed in this model is attained an improved transmission using TCP compared with the protocol used by GUWAL. GNUradio, a SDR defined one which is a medium of creation of covert channel and as of transmitting of data bytes which are a piece of malware code embedded into the TCP headers. To avoid such illegal or undefined way of communication as of operating systems and standardized hardware techniques, it's better to have Low Pass Passive filtering neither in software or hardware. In this architecture of sending data bytes using TCP is achieved, and further future implementations of using image file as source using steganography to send data securely not as for infection purpose.

REFERENCES

[1] Michael Hanspach and Michael Goetx, "On Covert Accoustical Mesh Networks in Air", Frauhofer FKIE, Wachtberg, Germany, arXiv:1406.1213v1 [cs.CR] 4 June 2014.

[2] Sverre Holm, "Hybrid Ultrasound – RFID Indoor Positioning Combining the Best of Both Worlds", *Senior Member, IEEE*, 2009 IEEE International Conference on RFID.

[3] Chuan Li, David A. Hutchins, and Roger J. Green, "Short – Range Ultrasonic Communications in Air Using Quadrature Modulation", *Senior Member, IEEE*, IEEE Transactions on Ultrasonics, VOL. 56, No. 10, Oct 2009.

[4] Boris Panajoto and Aleksandra Mileva, "Covert Channels in TCP/IP Protocol Stak", University "GoceDelcev", ICT Innovations 2013 Web Proceedings ISSN 1857 – 7288.

[5] Feng Ge, C. Jason Chiang, Yitzchak M. Gottlieb, and Ritu Chadha, "CNU Radio – Based Digital Communications: Computational Analysis of a GNSK Transceiver", Piscataway, NJ 08854, USA.

[6] Jakob Sloth Nielsen and Bjarke Freund-Hansen, "SDR Platform for Wireless Cooperative Protocols", Thesis accepted and used in Fall 2009 & Spring 2010.

[7] Steven J. Murdoch and Stephen Lewis, "Embedding Covert Channels into TCP/IP", www.cl.cam.ac.uk/users/{sjm217, sr132}/

[8] Kapil Singh, SamritSangal, Nehil Jain, Patrick Traynor and Wenke Lee, "Evaluating Bluetooth as a Medium for Botnet Command and Control", Georgia Institute of Technology.

[9] "Covert Channels Over Social Networks", SANS Institue InfoSec.

ISSN: 2278 – 1323