ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

An Approach to Secure Air-gap system from Intentional Radio Transmission

***Gaurav Neelwarna[1] and Dr. S. Magesh[2]**

1. M. Tech. Student, Faculty of Engineering and Technology, SRM University, Chennai, India.
2. Assistant Professor, Faculty of Engineering and Technology, SRM University, Chennai, India.

Manuscript Info

Manuscript History:

Received: 16 March 2016
Final Accepted: 26 April 2016
Published Online: May 2016

Key words:
Air-gap system. Covert channels, Frequency Modulation, Pixel clock or Dot clock, Harmonics, Jamming.

Corresponding Author

Gaurav Neelwarna.

Abstract

Air-gap approach is widely used for critical information systems. This approach gives us illusion that our data is secure from any potential attacks and data leakage. But, there are few covert channels which can be used to attack these systems.
Intentional Radio Transmission from video signal of system is one of such attack. In this attack transmitter code executing on air-gap system will generate Radio Signals at specific frequency, which will be received by nearby radio receiver device. In this paper, we tested this attack scenario and propose a technique to secure from such transmissions.

Introduction:-

Over a couple of decades computation and communication devices have grown vertically and horizontally. Computers provide wide range of protocols to transmit data, such as Ethernet, infrared, Bluetooth and Wi-Fi. In past lots of methods were developed and still being developed to stop data exfiltration from these channels. However, securing covert channels have been fallen off the radar. Covert channel allows the communication of information by transferring data through existing information channels that are not supposed to be allowed to communicate.

Almost all organizations rely on computer network; such networks connected to Internet are vulnerable to outside hacking. Irrespective of system and network security, attacker will eventually find a way to exfiltrate data. To avoid such events, industries that deal with sensitive information rely heavily on air-gapped systems. An air-gap is a security measure to protect critical data by keeping computer system or network isolated from external world, either directly or indirectly. However, these systems are more secure than the others, it has been proven that there are ways to compromise them, allowing attackers to steal highly sensitive data. Recent examples of Stuxnet and Agent.btz attacks show that attacking secured air-gap systems is practically possible.

Man-machine interface cannot be encrypted, so they are potential security risks. In [2], it has been proven that electromagnetic radiation emitted from video Display Units are similar to radio waves and that they could be intercepted.

Electromagnetic emission level has been kept low by International Standards concerning electromagnetic compatibility to prevent Electromagnetic Interference (EMI) from each other. All electronic devices which are fitted with LCDs emit some kind of Electromagnetic radiation (EMR) even though they are not designed to do so. These emissions can be intercepted by a remote receiver system by virtue that EMR in free space can be intercepted [1]. Our research focus is to implement this data exfiltration attack considering SDR (Software Defined Radio) as receiver and propose security mechanism for such attack.

Previous Research:-

System administrators may choose air-gap security measure to protect control-centers of critical infrastructure in order to protect data from attacks. Unfortunately, no system is 100% secure and researchers have proved various ways to breach it.

In [3], researchers introduced concept of "Audio Networking", to transmit data using inaudible data transmission. [4], discusses covert acoustical mesh networking. [5], presents software based hidden data transmission using electromagnetic emanations. [6], shows how to estimate amount of information that is leaked as electromagnetic emanation and effectiveness of averaging technique for reconstruction of displayed images. [7], gives estimation of the maximum receivable distance for the radiated emission. [8], analyzes quality of reconstructed display images with respect to font size and distance from receiver. [9], demonstrates a method of bridging the air-gap between adjacent compromised computers by using their heat emissions and built-in thermal sensors to create a covert communication channel. [10], discusses bridging air-gap system by intentionally creating FM (Frequency Modulation) radio emissions from a Video Display Unit which will be received by nearby mobile phone FM receiver, and this received signal will be further decoded into original data.

Wide use of modern mobile phones with FM radio receivers makes this scenario increasingly common. With appropriate software, compatible radio signals can be produced by a compromised computer, using the electromagnetic radiation associated with the video display adapter. The combination of a transmitter with a widely used mobile receiver creates a potential covert channel that is not being monitored by ordinary security instrumentation [10].
In this paper we propose a method to deny successful data transmission generated by radio emissions from Video Display Units.

Attack Implementation:-

Lots of researchers have discussed radio signal generation from Video cards [1], [2], [5], [10], [11], [12]. Data intentionally modulated on these video signals will be transmitted by computer's monitor cable. Here, monitor or monitor cable will act as antenna. FM receiver will collect the transmitted signals and extract the modulated data.

Attack Model:-

To transmit data from air-gap system, attacker should breach the system to install hostile code. Possible attack vectors are (a) through removable media or (b) through outsourced software or hardware components [10]. In the case of Stuxnet, removable media acted as propagation framework [13].

FM Transmitter:-

To determine at what frequency signal should be transmitted, we need to determine pixel clock and sync values of display adapter.
Pixel clock is the frequency at which pixels are transmitted per second through video card. It is calculated as

$$PC = (H_{Total})(V_{Total}) (RR \ \ )$$

where, H_{Total} is addition of Horizontal resolution and horizontal sync pixels which are not illuminated, V_{Total} is addition of Vertical resolution and vertical sync pixels which are not illuminated, RR is Refresh Rate, PC is Pixel Clock. In Linux, xvidtune utility is helpful to determine these values. To test data transmission by emanating radio waves from Video Displays, we used variant of code from Tempest for Eliza [10], [11]. To improve quality of transmitted signals we reduced Horizontal and Vertical sync times as per [12].
It generates pixel pattern that cause emission of specific FM signal. For audio modulation, signal is generated at carrier frequency, which is limited to less than half of pixel clock of display. Since video displays are Digital-to-Analog Converters they generate a lot of harmonics. We can use this property to get our signal up to the FM band if we are unable to directly generate FM carrier [12]. The Signal will be weak compared to the signal received at carrier frequency. For example, if PC denotes pixel clock frequency and Fc is carrier frequency then the harmonics will appear at n*PC + Fc for all integer values of n.

FM Receiver:-

Now days, all smartphones have FM receivers. Guri [10] consider use of mobile phones as an intended receiver. Since everyone is using mobile phones, attacker can consider using them.To test the reception of generated signal, we implemented FM receiver in GNU Radio [14] using RTL SDR (Software Defined Radio) Stick [15]. SDR Stick is very cheap available at market price of $10. Fig. 1 shows attack model setup.

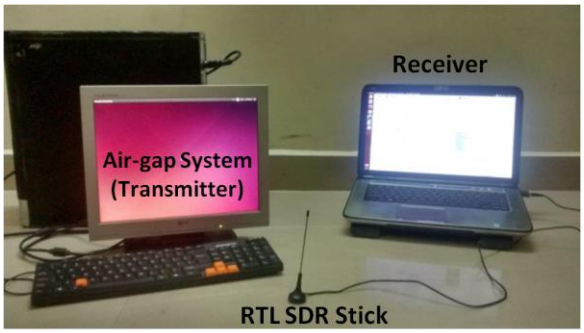

Fig. 1 Attack Model

Security Measures:-

Conventional Security Measures

Suzuki and Akiyama [16] discuss conventional counter measure techniques to prevent information leakage from PC via Video Signals and also proposed a jamming technique to shield from such intrusions. The simplest method is to shield devices, rooms, specific floors, or buildings with metallic materials. This method is quite expensive for shielding large area.

Kuhn [5] suggests that strength of emissions can be reduced using specifically designed fonts, which are available through Soft Tempest.

Zoning is a policy driven security measure for maintaining a certain distance between air-gapped system and possible eavesdroppers. This enables us to select proper countermeasure based on the protection level defined in each zone.

Jamming is a technique in which random noise or meaningless signals overlays on the original emanation in order to prevent interception of the leaked information.

A combination of these schemes would be an effective overall countermeasure [16].

Two types of standards exists US NACSIM 5000 and NATO SDIP-27 which can protect from intentional radio transmission attack on air-gapped systems, but these standards are classified [17].

Proposed Jamming Scheme

To prevent information leakage from air-gapped system we propose a jamming scheme.To feed the same VGA signal to jamming circuit we used VGA splitter cable. As shown in Fig. 2, one output of cable is connected to monitor and another to jamming circuit.

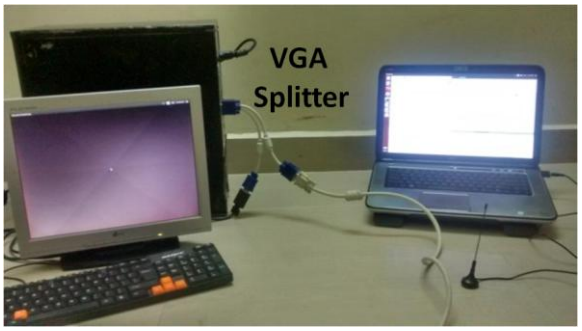

Fig. 2 Jamming Scheme Setup

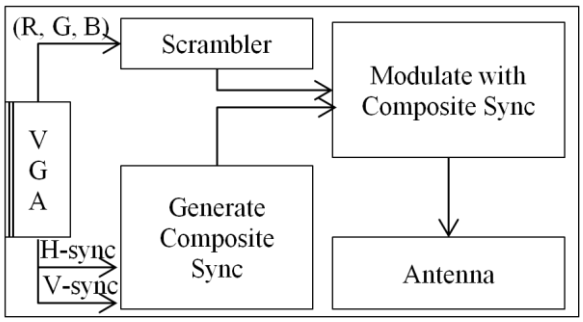

Fig. 3 Layout of Proposed Jamming Scheme

Fig. 3 shows function diagram of the circuit. It generates composite synchronization signal from Horizontal Synchronization (H_{Sync}) and Vertical Synchronization (V_{Sync}) [18]. Scrambler modifies input signal randomly and generate jamming signal. So whatever frequency a transmitter is generating, we have jamming signal for the same frequency. Next we modulate jamming signal with composite synchronization signal. To obstruct receiver from FM signal, its level should be sufficiently higher than FM signal. Finally modulated signal is fed to antenna.

Performance Evaluation:-

Setup:-

We used Pentium IV machine as Air-gapped System with 32-bit Ubuntu-14.04.3, kernel 3.19.0-25-generic. FM Receiver was implemented on Dell XPS Laptop with 64-bit Ubuntu-14.04.3, kernel 3.19.0-generic with help of SDR Stick. For connecting monitor and circuit with air-gapped machine we used Standard (shielded) VGA cable and VGA Splitter.

Results:-

In normal scenario, as the distance of receiver from transmitter increases received signal strength will decrease. We measured power of received signal using GNU Radio FFT plot across varying distances. Graph in Fig. 4 summarize these results.

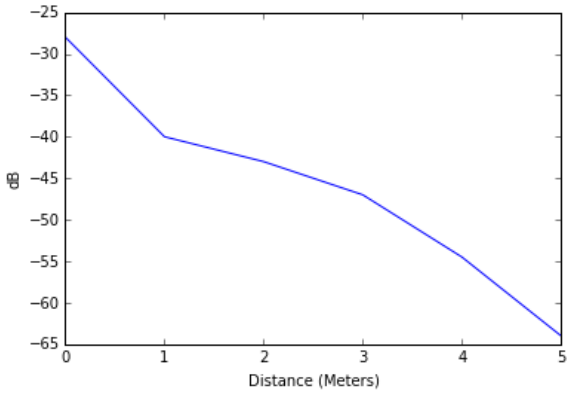

Fig. 4 Signal Strength with respect to distance

Based on above tests, we found that maximum receivable distance is 4 meter for RTL-SDR USB Stick receiver.

Conclusion:-

We successfully tested intentional radio transmission by video signal using GNU Radio and RTL-SDR as receiver. The idea behind proposed jamming design is that it should generate jamming signal only for intentional transmission signal frequency and not jam whole range of possible set of frequencies, and avoid jamming other legal signals. The proposed jamming scheme implementation may vary, and we leave it for future work.

References:-

1. K. A. Ghani, K. Dimyati, K. Ismail and L. S. Supian, "Radiated Emission from Handheld Devices with Touch-Screen LCDs," *Intelligence and Security Informatics Conference (EISIC), 2013 European*, Uppsala, 2013, pp. 219-219.
2. W. van Eck. "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," *Computers & Security 4*, 1985, pp. 269-286, 1985.
3. Madhavapeddy, R. Sharp, D. Scott and A. Tse, "Audio networking: the forgotten wireless technology," in *IEEE Pervasive Computing*, vol. 4, no. 3, pp. 55-60, July-Sept. 2005.
4. M. a. G. M. Hanspach, "On Covert Acoustical Mesh Networks in Air,"*arXiv preprint arXiv:1406.1213*, 2014.
5. M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden data transmission using electromagnetic emanations," in *Information hiding*, Springer-Verlag, 1998, pp. 124-142.
6. H. Tanaka, "Information Leakage via Electromagnetic Emanation and Effectiveness of Averaging Technique," *Information Security and Assurance, 2008.ISA 2008.IntentionalConference on*, Busan, 2008, pp. 98-101.
7. H. Sekiguchi and S. Seto, "Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 55, no. 3, pp. 547-554, June 2013.
8. F. Elibol, U. Sarac and I. Erer, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system," *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*, Bucharest, 2012, pp. 1767-1771.
9. Mordechai Guri, MatanMonitz, YisroelMirski, Yuval Elovici, "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations", Available: http://arxiv.org/abs/1503.07919.
10. M. Guri, G. Kedma, A. Kachlon and Y. Elovici, "AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies," in *9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014)*,Puero Rico, Fajardo, 2014.
11. E. Thiele. "Tempest for Eliza." 2001, [Online] Available: http://www.erikyyy.de/tempest/.[Accessed July 2015].
12. B. Kania, "VGASIG: FM radio transmitter using VGA graphics card," 19/4/2009. [Online]. Available: http://bk.gnarf.org/creativity/vgasig/vgasig.pdf. [Accessed July 2015].
13. S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," *IECON 2011 - 37th Annual Conference on IEEE Industrial Electronics Society*, Melbourne, VIC, 2011, pp. 4490-4494.
14. GNURadio. [Online]. Available: http://gnuradio.org/redmine/projects/gnuradio/wiki. [Accessed December 2015].
15. RTL-SDR.COM Quick Start Guide. [Online]. Available: http://www.rtl-sdr.com/rtl-sdr-quick-start-guide/. [Accessed December 2015].
16. Y. Suzuki and Y. Akiyama, "Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals," *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium on*, Fort Lauderdale, FL, 2010, pp. 132-137.
17. Tempest (codename). [Online]. Available: https://en.wikipedia.org/wiki/Tempest_(codename). [Accessed August 2015].
18. VGA to RGB + composite sync -converter Designed by Tomi Engdahl. [Online]. Available: http://www.epanorama.net/circuits/vga2rgbs.html. [Accessed February 2016].