iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XII **Month of publication:** December 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Vulnerabilities Analysis of WI-FI Networks

Aaina, R. M Singh
Post graduate (C.S.E), India, DRDO, India

Abstract— Modern surveillance devices are increasingly being taken off private networks and placed onto networks connected via gateway to the Internet or into Wi-Fi based local area wireless networks (LAWN). The devices are also increasingly using IPv4 and IPv6 network stacks and some form of embedded processing or compute built in. Additionally, some specialist devices are using assistive technologies such as GPS or A-GPS. This paper explored the issues with use of the technologies in a networked environment, both wireless and internetworked. Analysis of these systems shows that the use of IP based CCTV systems carries greater risk than traditional CCTV systems, primarily due to the exposure to IP based vulnerabilities. Furthermore, Wi-Fi based IP CCTV systems are additionally susceptible to remote, physical denial of service attacks due to the broadcast nature of wireless communication systems. Interception of traffic is possible with IP based systems, and again,Wi-Fi IP based CCTV systems are more susceptible due to protocol vulnerabilities and lack of processing power. The paper concludes that more research is needed in this area to identify and classify generic vulnerabilities that these systems are vulnerable to, and to present a framework which can be used to mitigate the risk of adopting these systems.
Keywords— Wi-Fi, CCTV, security, LAWN, IP

I. INTRODUCTION

There continues to be a prolific expansion in the use of technological surveillance infrastructures in the public and private domains and it was also emphasised that the integration of traditional surveillance devices (CCTV, microphones, motion detectors) are increasingly utilizing embedded compute environments, with Wi-Fi and IP network connectivity to provide extended feature sets and provide data feeds for integration with modern security event management systems.Yet many embedded devices are built with security of the device itself being largely ignored. The weakness in embedded systems security has been adequately demonstrated by various breaches of embedded systems in existing implementations and usage, including parking meters, hotel door systems, and smartgrid electricity control systems. One of the key differences between conventional compute versus embedded weaknesses is that in some instances compute can be patched over. However, an embedded system normally has immutable software burned into hardware that is difficult or unable to be updated, thus leaving the device vulnerable to attack or compromise. Should a vulnerability be discovered in an embedded device, the only solution would be to replace the device or entire system which incorporates that device if it is an essential component. Depending on the extent and impact of the embedded vulnerability, it may be a significant undertaking from the perspective of cost and time to replace vulnerable equipment.Wireless enabled devices and related network protocols have also been found to be highly insecure. Wireless technology has consistently proven itself vulnerable to physical attack methodologies via the use of physics of wireless transmission. Because the vulnerabilities lie in the lower layers of the protocol, it is irrelevant as to whether the information being transmitted is email, webpages, music, images or video. Due to this the use of radio waves as the medium of transmission, it has also been demonstrated that signals between entities in that network are highly susceptible to attack via interception of or denying the transmission of video captured streams can then be later decoded and viewed at will, and once the encoding/decoding(codec) has been determined for the video stream, there is the potential for it to be viewed in real time. The aim of this paper is to firstly explore the role of CCTV, and the increasing implementation of Wi-Fi based CCTV systems. The vulnerabilities which exist in Wi-Fi networks are examined, with a focus on the implications for CCTV systems. This is done using the confidentiality, integrity and availability model used ininformation security, as ultimately, CCTV video streams are just another form of information. Finally, a framework is presented indicating appropriate controls which should be implemented to lower the level of risk associated with the use of CCTV.A closed circuit television society Contemporary society has accepted the prolific expansion in the use of surveillance infrastructures in the public and private domains.

II. ISSUES WITH SECURITY OF NETWORKED SURVEILLANCE DEVICES

It is expressed a general theme that security's role is to manage the threats which pose a risk, which if accepted means the threat focus must also be steered towards the threats which pose a risk to the internal validity of the mitigation systems (technologies) themselves. Yet at present much of the current debate embodying the use of CCTV is significantly focused towards the socio-economic, legal, fiscal, and political contexts. However, most authors have expressed concerns about security of the transmitted

digital video signals. Yet many consider that the tools available can overcome transmission medium vulnerabilities. For example, when considering the security of video stream over an intranet or internet connection per ports that such vulnerabilities can be overcome through user name and login requirements, enhanced through the use of encryption protocols. Within the wireless topologies providers that traffic filtering and VirtualLAN provisions coupled with strong encryption (256 bit keys for Advanced Encryption Standard (AES)) block any unauthorized traffic from manifesting threats against the system. Nevertheless, vulnerabilities within the advanced transmission mediums exist which if exploited can have catastrophic effects in relation to the timing of attacks or interruptions accordant with surveillance field of view objectives at that time. One means of assessing the impact of an exploitation of the various vulnerabilities present in both the wireless protocols and the devices themselves is to examine it from an information security perspective. There are three fundamental principles of information security which relate to the protection of information assets. These are confidentiality, integrity and availability (CIA) of data. These can further be devolved into six sub-categories, but for the purposes of examining Wi-Fi CCTV issues, the vulnerabilities will be classified using the CIA core principles.

Data confidentiality refers to who can see the information, and can the information be protected such that others cannot see it? Confidentiality is difficult to guarantee with wireless transmissions, as now with minimal technological knowledge, skills and resources low threat adversaries can pick up the signal due to it being a broadcast radio. Whilst the ability to encrypt transmitted data exists, encryption reduces the amount of data that can be transmitted. In the case of video, this means lower quality video or less frames per second, neither of which is desirable if the images were to be used for identification purposes. In addition, wireless encryption is not invulnerable: it can be broken, and the video feed can be captured.Data integrity refers to whether the data can be changed while it is being transmitted, and it also covers the issueof whether the signal we receive is coming from our camera. Integrity relates to a very real risk of foreign data being injected into a Wi-Fi system, and a greater risk of someone hijacking the signal. It can be difficult to prevent either of these attacks from occurring due to the availability of commercial technologies and supporting software.

Data availability refers to whether you can access the system, and although last of the three, this is the most critical when it comes to a surveillance system – if it becomes unavailable, it is of no use. Unfortunately, wireless networks are extremely vulnerable to denial of service attacks, and there is no way to prevent such an attack from occurring because Wi-Fi is an open system. A denial of service attack literally means that someone prevents you from being able to use the system. Since there are so many other people using Wi-Fi frequency band there is always going to be some level of interference. It is a trivial task to prevent a Wi-Fi device from being able to communicate with a base station. There are free tools available on the internet which can be downloaded and used with very limited capability. There are even videos available which show novices how to use the tools to attack Wi-Fi networks. The weather can also cause a denial of service attack. As the frequency used is absorbed rapidly by water, rain can greatly reduce, or even stop the signal if it is heavy enough.

Understanding Wi-Fi protocol based vulnerabilities in transmission protocols on CCTV Field of view objectives, there are a number of specific categories of vulnerability as it relates to Wi-Fi based CCTV implementation which can impact in terms of the CIA approach. One category relates to the use of wireless networks as the transmission medium between camera and recorder / collector. One aspect in this category is that wireless is a broadcast medium, meaning that the information is effectively broadcast and propagated over a wide area where a suitably equipped entity within the signal locus can be capable of capturing this information. Another aspect is embedded vulnerabilities in the modus operandi of the 802.11 protocol and the extensions to this protocol. The inability to verify management and control frames is one such vulnerability, leaving the network susceptible to Denial of Service (DoS) and man-in-the-middle (MITM) attack. In addition to issues relating to the use of wireless, and Wi-Fi in particular, are vulnerabilities embedded in the firmware of the camera systems themselves (Metasploit, 2012). Whilst not as widespread as the broad spectrum issues with Wi-Fi, such vulnerabilities can be difficult to mitigate as there are specific vulnerabilities associated with the transmission of video data over Wi-Fi networks leaving such systems open to exploitation. This includes issues with encryption, authentication as well as vulnerabilities associated with the wireless medium itself.

III. EAVESDROPPING – (CONFIDENTIALITY)

The functionality of Wi-Fi networks also presents one of its biggest problems in terms of vulnerability to exploitation. Since wireless is a broadcast medium, there is no way to control where the information is sent and who therefore has access to it. By modifying the drivers used with the Wi-Fi client devices, many individuals and organizations have developed analysis tools, known as “sniffers”. There are both freeware (Kismet) and commercial (Airopeek) versions of this type of software (Berghel and Uecker

2004). When used within the broadcast range of a Wi-Fi network, these can be used to capture every packet travelling the Wi-Fi network. If an access point is set up and used in its default configuration, then the user of such a system is vulnerable to attack, because anyone running sniffer software can see and capture everything that a user does across that network. This includes data (medical records), passwords and email messages. Even when encryption is used, there is still important information which is available to anyone within range of a Wi-Fi network. This includes the network name, known as the SSID, the MAC addresses of both AP and clients and a range of other information. Both Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are security features intended to provide a level of security for Wi-Fi networks which was the equivalent to that of wired networks.Unfortunately, the implementation of the RC4 cipher meant that the WEP key can be discovered in as little as >5 minutes by an attacker, and all traffic from a Wi-Fi camera to an access point could be captured and viewed.

The WPA security protocol was designed and implemented as a replacement for WEP. Unfortunately, reuse of some aspects of WEP means that implementation of so called WPA personal using a secret key is also vulnerable to attack and key discovery. An attacker need only capture the SSID, which is broadcast in the clearby Wi-Fi network devices, and using a GPU based computer can break the WPA key in a matter of days.

IV. PROTOCOL LAYER VULNERABILITIES

A. *Layer 1 (Physical jamming) – (Availability)*

A layer 1 or jamming attack is reasonably easy to perpetrate, and also reasonably difficult to detect. Such a system attack can be either intentional or unintentional. Recent testing supports that an intentional attack where an interloper broadcasts a very high-power signal at the same frequency that theWi-Fi network is operating on, causing interference to the network. In addition, testing also supports that such an attack may also occur unintentionally, through the action of placing a device which operates at the same frequency in the vicinity of the Wi-Fi network. For devices that operate in the 2.4GHz frequencies, this includes microwave ovens, some cordless phones, baby monitors and Bluetooth devices. Bluetooth devices are known to interfere with the operation of Wi-Fi networks.

B. *Layer 2 (Logical jamming)*

Layer 2 attacks exploit the lack of verification of control frames in Wi-Fi networks. As this control and management information is a broadcast in the clear by Wi-Fi networks, testing has shown that it can be captured by an attacker using a freely available packet capture tool, such as Kismet (Berghel and Uecker 2004). Once gathered this information can then be used against the Wi-Fi network that it was captured from and used to disassociate or de-authenticate a valid client from the network. This type of attack is probably one of the most concerning to IS managers as there appears to be no adequate means to prevent it from occurring.

V. SIGNIFICANCE OF VULNERABILITY EXPLOITATION IN WI-FI CCTV BASEDSYSTEMS

Closed Circuit Television (CCTV) has been embraced as the panacea of many societal, organizational and personal surveillance concerns. To this end, much of the transmission of digital video image is occurring through both internet protocol (IP) cameras and Wi-Fi transmission technologies. As the roles and functions of CCTV vary so does the direct impact of attacks against the transmission infrastructure. As a video stream is simply another form of information, it is appropriate to use the confidentiality, integrity and availability (CIA) model, as described in the information technology security evaluation criteria (ITSEC) methodology and used extensively in software and other IT systems. Accordant with the CIA model of information security the impact of exploitation of each aspect is as contextual as thesurveillance objectives.

A. *Confidentiality*

For data transmission protocols a feasible attack methodology was highlighted to be the man-in-the-middle(MITM) attack, where a third party is able to intercept a Wi-Fi camera feed and uses it to their own ends. It is also emphasised the term closed refers to the fact that the system (CCTV) should only be accessible by equipment within the system. However, testing has supported that concern that the man-in-the-middle (MITM) attack can result in outsiders gaining access to the streamed video image, or may achieve access to command and control functions. In such circumstances analyses of streamed video signal can facilitate an understanding of actual field of view coverage to ascertain where camera blind spots exist. This information can be used by adversaries in their attack planning stages. Such an attack could impede against the core principles of availability, confidentiality and integrity of transmitted data. Thus an attacker who is able to gain a level of unauthorised access may be able to monitor the environment using the CCTV system as their personal surveillance and intelligence collection medium to plan an attack at the time where they believe the chances of being detected are low, the difficulty in attacking is low and the chances of being caught are low (rational Choice). Additionally,

in contemporary times attackers may choose to intercept a CCTV video stream of an incident from a Wi-Fi camera.

B. Integrity

In addition, system interlopers may be able to alter network settings which would benefit their advances against a physical protection system (PPS). Testing has supported that attackers can set up a fake cameras and record CCTV video streams of your environment during stable operating times. Then they can configure their technology to communicate with your system and broadcast a pre-recorded loop showing normal activity during intrusion events, reducing alarm assessment efficacy and situational awareness. Again, such attacks provide a window of opportunity to attack either a PPS or a surveillance environment due the heavy reliance of the CCTV footage in guard force decision making. Furthermore, little research has been undertaken on the admissibility of recorded vision as evidence when such an attack occurs. Recent testing provides sufficient evidence of problems with Wi-Fi networks such that it may possible to introduce reasonable doubt into the minds of jurors about whether captured video stream was indeed from a legitimate signal, or that it may have been interfered with at some point during transmission.

C. Availability

In considering the threats of compromising the availability of captured and transmitted data testing has identified that adversaries can conduct physical layer jamming actions against the Wi-Fi networks, effectively taking the cameras offline. As Garcia (2001) pointed out, the role of CCTV in perimeter security is alarm assessment where there is a requirement for operators to see fine details within the image when deciding if further response is required. If increasing trends towards Wi-Fi technologies continue and Wi-Fi CCTV is expanded to be used for alarm assessment across facilities, then the affects of a denial of service attack may provide the extra time required for an adversary to complete their attack path due to delays in effective alarm assessment. Furthermore, such an attack can have catastrophic consequences in emergency management responses. As authors pointed out, CCTV played a significant role in emergency response operations during the September 11, 2001 terrorist attacks. Attacks such as denial of service against transmission architectures during emergency situations can negatively impact on the decision making due to the removal of situational awareness. Such an attack would require personnel to moved closure to incident sites placing human lives at greater risk when such risks should be overcome through available engineering means. As such, where Wi-Fi connectivity is utilized, to overcome the vulnerability of single point failure additional transmission functionalities such as Infra-Red (IR) need to be integrated as redundancy measures at extra costs.Other concerns associated with reliable availability can stem from non malevolent actions where a user misconfigures their Wi-Fi network, or installs a new Wi-Fi network which interferes with your signal to such an extent that it dramatically reduces the frame rate so that your system effectively suffers reduced availability. This may manifest at the same time that an incident occurs resulting in cameras do not capturing what is required to aid decision making because the frames transmitted were either side of the key data. Such concerns can also occur during heavy rain showers which have the effect of reducing the signal to a point where no useful images are able to be viewed and recorded, again impeding timely decision making. For Wi-Fi camera systems to be effective the communication signal needs to be high enough in power output to ensure good connectivity. However, in boosting the signal to such levels you may interfere with other(also legitimate) Wi-Fi network users in the area resulting in their networks becoming unusable for them at keytimes requiring decision making as you have effectively created a denial of service attack against them.There are security concerns associated with those vulnerabilities in CCTV cameras hardware, software,firmware and device configuration. For example, the security testing tool Metasploit contains an exploit for a control protocol vulnerability in the Rosewill RXS-3211 IP camera which allows for password retrieval andsubsequent control of the camera (Metasploit 2012). The explanatory note that describes this vulnerability statesthat IP cameras from Edimax, Hawking and Zonet amongst 150 others are also likely vulnerable to the sameexploit. The author notes that as this is a protocol vulnerability, both firmware and software would need to be patched (Schmidt 2012). There are potentially large numbers of cameras vulnerable to this exploit due to the common practice of rebranding or re-badging a generic or licensed hardware platform. The Metasploit framework also carries a module which tests a range of CCTV DVR systems, including Micro Digital, HIVISION and CTRing amongst numerous others, to determine whether they are sill employing the default passwords (Metasploit 2012). The module also allows for brute force attacks against user accounts.

The software is known to use port 5920/TCP for authentication and the system is known to stream video over 5921/TCP. It is unclear as to whether these default ports can be changed. Furthermore, management control of the actual devices themselves is often done via inherently weak protocols to access the control interfaces that transmit details using plain text (human readable) across a network. Plain text transmissions are readily readable. The actual daemons or servers that run on such management consoles on the

embedded systems suchas http (port 80) or telnet (23) can have inherent weakness in them as well that is once again typically immutablefor the life of the device. Some systems will also provide management interfaces on desktop operating systems with little or no vendor updates.

Software obsolescence and obfuscation are problems for the actual devices in particular CCTV cameras. These cameras have specific software called a codec for coding and decoding of images that may only work with the particular hardware and software supplied by the vendor. The software is rarely updated and hence becomes locked into a particular operating system which overtime will become insecure. This fact is evince by the fact that no current and legacy modern desktop based Windows, Linux or Macintosh system is vulnerability or remote exploit free. Exploitation of the vulnerability will allow an intruder often to take over command and control of the desktop operating system and therefore via chained logic all applications on that system.

VI. FRAMEWORK FOR REDUCING RISK OF WI-FI CCTV SYSTEMS

Although attacks in the availability category cannot be prevented or mitigated, there are some controls which can be implemented to lower the risk of Wi-Fi CCTV based use in terms of confidentiality and integrity. The framework presented in Table 1 is based on a meta analysis of publications in relation to Wi-Fi security, theIEEE 802.11i security protocol extension, and the certified wireless security professional (CWSP) industry best practice certification. The category of attack is listed using CIA, relevant controls are listed, and their effect onrisk is given. While a control is presented for availability attacks, the risk level associated with the threat of denial of service attacks remains significant.

TABLE 1: A FRAMEWORK FOR IMPLEMENTING CONTROLS TO REDUCE RISK ASSOCIATED WITH WI-FI BASED CCTV SYSTEMS.

	Attack	Control	Impact on risk level
Confidentiality	Interception of signal	AES encryption*1	Significant reduction
Integrity	Man in the Middle	Virtual Private Network (VPN)	Reduction
	Broadcast of false signal	802.1x authentication	Significant reduction*2
		MAC address locking	Reduction
Availability	Denial of Service (Physical)	Triangulate jamming signal and shut down*3	Negligible reduction
	Denial of Service (Logical	Locate device and attempt to shut down*4	Negligible reduction

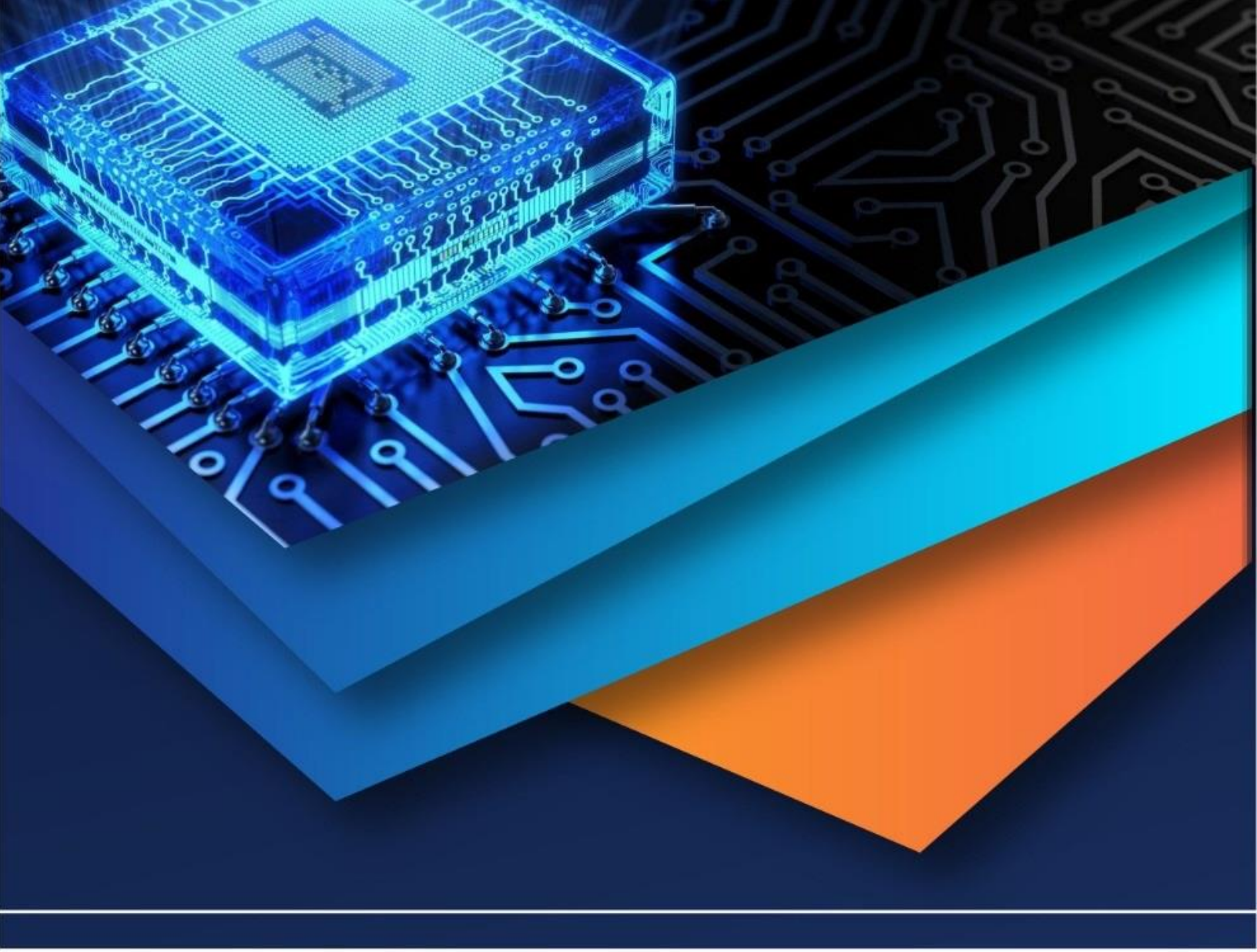
A. This may have an adverse impact on the system as processing power is required for encryption / decryption
B. This type of authentication may not be available on Wi-Fi CCTV systems
C. This would be post incident and would not prevent an attack
D. This would be post incident, and if the device is inadvertently jamming, it may not be possible to shut down

VII. CONCLUSION

Many organizational teams are recommending the move from traditional cable centric CCTV transmission mediums to less costly Wi-Fi technologies, but such technologies are not without their security concerns. This article has highlighted a number of issues with the use of Wi-Fi based CCTV systems, which can be attributed to the use of radio frequency as the physical transmission system. There are a number of significant conclusions, which can be drawn from this paper. Firstly, the use of Wi-Fi CCTV systems introduces significant vulnerability into what were previously closed systems. Secondly, the vulnerabilities and threats to Wi-Fi CCTV differ fundamentally from traditional cable based systems. Adopters of Wi-Fi CCTV need to understand that they are doing so from a cost benefit and convenience perspective, not a security one. Accordant with the CIA model of information security there exists increased security vulnerabilities of such systems where audit tools such as the Metasploit Framework already incorporate modules which can be used to compromise a wide range of CCTVand IP based camera systems. Secondly, further research needs to be undertaken to classify the use of such IPbased systems, and to catalogue the existing and potential vulnerabilities within such systems. There is currently a significant lack of published research in this field, and a subsequent lack of guiding information for adopters of these systems. Given the array of embedded vulnerabilities with Wi-Fi as outlined in this paper, organizations need to conduct strict and thorough risk assessments before deploying Wi-Fi surveillance systems based on the surveillance contexts and the significance of attacks against their Wi-Fi networks.

REFERENCES

[1] Atlas, R., I. (2008). 21st Century Security and CPTED: Designing for critical infrastructure protection and crimeprevention. CRC Press. New York.
[2] Brooks, D., J. (2011). Intelligent buildings: An investigation into current and emerging security vulnerabilities in automated building systems using an applied defeat methodology. Proceedings of the 4th Security andIntelligence Conference.
[3] Clarke, R., V. (1992). Situational Crime Prevention: Successful case studies. Harrow and Heston. New York.
[4] Coole, M. & Brooks, D., J. (2011). Mapping the organisational relations within physical security's body of knowledge: A management heuristic of sound theory and best practice. Proceedings of the 4th Security andIntelligence Conference.
[5] Garcia, M. L. (2001). The design and evaluation of physical protection systems. Butterworth Heinemann.United States of America.
[6] Hafiz, M., P. Adamczyk, et al. (2007)."Organizing Security Patterns." Software, IEEE
[7] Huyu, Q., C. Jie, et al. (2009). WiFi-Based Telemedicine System: Signal Accuracy and Security. Computational
[8] Science and Engineering, 2009.CSE '09. International Conference .24(4): 52-60.
[9] Irvine, C. and T. Levin (1999).Toward a taxonomy and costing method for security services. Computer Security
[10] Kerner, S. M. (2012). "Black Hat Hacking Hotel Doors With Open-Source Arduino." Retrieved August 22nd,
[11] Koopman, P. (2004). "Embedded system security." Computer 37(7): 95-97.
[12] Kruegle, H. (2007). CCTV surveillance: Anologue and Digital Video Practices and Technology. 2nd ed.Elsevier. United States of America.
[13] Marco Domenico, A., C. Giorgio, et al. (2007). "Dependability in Wireless Networks: Can We Rely on WiFi?"Security & Privacy, IEEE 5(1): 23-29.
[14] Musaloiu-E, R. and A. Terzis (2008)."Minimising the effect of WiFi interference in 802.15.4 wireless sensornetworks." International Journal of Sensor Networks 3(1): 43-54.
[15] Norris, C., McCahill, M., & Wood, D. (2004). The growth of CCTV: A global perspective on the internationaldiffusion of video surveillance in public accessible space.
[16] Pelechrinis, K., M. Iliofotou, et al. (2011). "Denial of Service Attacks in Wireless Networks: The Case ofJammers." Communications Surveys & Tutorials, IEEE 13(2): 245-257.
[17] Taylor, E. (2010). Evaluating CCTV: Why the findings are inconsistent, inconclusive and ultimately irrelevant.Crime Prevention and Community Safety. 12 (4), pp 209-232.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY