ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Design and Detection of Covert Timing Channels and Spyware Using Warden Technique

C.Logasundari[1], V.Menaka[2], R.Madhubala[3], G.Misal[4]

V.S.B.Engineering College, Karur, Tamilnadu, India[1, 2, 3, 4]

Abstract: Dependence on the internet is growing and so is the dangers related to it are focusing for past decade. Viruses, Trojan horse and malware are some spyware threatening the security of web. The cyber sphere is what one would call a double-edged sword. While it brings the world closer with easy information and fast communication, it also poses serious problems that threaten your online presence and computer system. Many researches are focusing in spyware detection and trying to clear those malware after affect the system. Moreover, spyware is a program that is put in someone's computer secretly to gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. If the spyware attacked system send message to anybody, then the copy of the message can be send to spyware activator. It is illegal process. It can easily retrieve the secret information. Our proposed work, focus not only in detecting the spyware initiator but also identifying the initiator. We use the warden technique; it can detect the spyware using timing channels that can identify the initiator who is in that covert communication. Our work mainly focused on information security on web. The CSMA/CA also used to identify the spyware software.

Index Terms: Timing channels, Covert communication, Warden Techniques, Information security.

I. INTRODUCTION

Information security is the protection of data saved to a network or hardrive. It is extremely easy to utilize. For protection of less sensitive material users can simply password protect files. For the more sensitive material users can install biometric scanners, firewalls, or detection systems. It keeps vital private information out of the wrong hands. Information security protects users valuable information both while in use and while it is being stored. The internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection. Thus, individuals and organization scan reach any point on the internet without regard to national or geographic boundaries or time of day. However, along with the convenience and easy access to information come risks. Among the mare the risks that valuable information will be lost, stolen, changed, or misused. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home; they may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can also create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

An information security policy usually has the following objectives:

1. To protect the organizations information by safeguarding its confidentiality, integrity and availability.
2. To establish safeguards to protect the organization's information resources from theft, abuse, misuse and any form

of damage.

3. To establish responsibility and accountability for information security in the organization.
4. To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of information security incidents.
5. To ensure that the organization is able to continue its commercial activities in the event of significant information security incidents.

II.RELATED WORK

Negar Kiyavash et al :"A Timing Channel Spyware for the CSMA/CA Protocol"(2013)The design and implementation of spyware communication circuits built into the widely used carrier sense multiple access with collision avoidance (CSMA/CA) protocol. The spyware components are embedded within the sequential and combinational communication circuit structure during synthesis, rendering the distinction or dissociation of the spyware from the original circuit impossible. We take advantage of the timing channel resulting from transmission of packets to implement a new practical coding scheme that covertly transfers the spied data. Our codes are robust against the CSMA/CA's random retransmission time for collision avoidance and in fact take advantage of it to disguise the covert communication. The data snooping may be sporadically triggered, either externally or internally. The occasional trigger and the real-time traffic's variability make the spyware timing covert channel detection a challenge. The spyware is implemented and tested on a widely used open-source wireless CSMA/CA radio platform. We identify the following performance metrics and evaluate them on our architecture: 1) efficiency of implementation of the encoder; 2) robustness of the communication scheme to heterogeneous CSMA/CA effects; and 3) difficulty of covert channel detection. We evaluate criterion 1) completely theoretically. Criterion 2) is evaluated by simulating a wireless CSMA/CA architecture and testing the robustness of the decoder in different heterogeneous wireless conditions. Criterion 3) is confirmed experimentally using the state-of-the-art covert timing channel detection methods.

Sedar cabuk:"IP covert timing channels: design and detection"(2012) A network covert channel is a mechanism that can be used to leak information across a network in violation of a security policy and in a manner that can be difficult to detect. In this paper, we describe our implementation of a covert network timing channel, discuss the subtle issues that arose in its design, and present performance data for the channel. We then use our implementation as the basis for our experiments in its detection. We show that the regularity of a timing channel can be used to differentiate it from other traffic and present two methods of doing so and measures of their efficiency. We also investigate mechanisms that attackers might use to disrupt the regularity of the timing channel, and demonstrate methods of detection that are effective against them.

Li Yang et al:"Real-Time Detection of Covert Channels in Highly Virtualized Environments" (2011) Despite extensive research, covert channels are a principal threat to information security. Covert channels employ specially-crafted content or timing characteristics to transmit internal information to external attackers. Most techniques for detecting covert channels model legitimate network traffic. However, such an approach may not be applicable in dynamic virtualized environments because traffic for modeling normal activities may not be available. Work describes that Observer, a real-time covert channel detection system. The system runs a secure virtual machine that mimics the vulnerable virtual machine so that any differences between two virtual system can be identified in real time. Unlike other detection systems, Observer does not require historic data to construct a model. Experimental tests demonstrate that Observer can detect covert channels with a high success rate and low latency and overhead.

Steffen Wendzel:"Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden"(2010) We definea building in the context of multilevel security (MLS) and show that covert channels and side channels exist in building automation. Additionally, we present a system called the building aware active warden to eliminate covert/side storage channels in building automation systems (BAS). Active wardens aim to remove malicious (covert) elements in communications and are a well-known means from the area of network covert channels and steganography. Within the last years, new models, such as the network-aware active warden, were developed. The presented building-aware active warden is an adoption of the concept of a network-aware active warden to building automation. Buildingaware active wardens modify or drop building automation commands as well as building information requests from users based on their security levels to enhance a building's security. We extended an interoperable system for building automation supporting hardware from two vendors for the purpose of a building-aware active warden and for providing an unified application programming interface.

III. EXISTING SYSTEM

A cognitive radio device is typically implemented by a general purpose computer processor that also runs radio application software. As a result, it is susceptible to spyware and malicious software or hardware. The existing hardware Trojan detection mechanisms are not able to detect our spyware because our assumptions are radically different. Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge. In existing it's not detected. Covert channels are mechanisms for communicating information in ways that are difficult to detect.

Disadvantages in existing system:

1. The spyware is protected in any node that not detected.
2. The spyware get the user data without our knowledge and give the data to third-party.
3. The covert communication not detected in normal hardware/software detection.
4. The CSMA/CA protocol results in random delays in the packet inter arrival times

IV. PROPOSED SYSTEM

We present a new transparent and robust covert communication scheme that can reliably spy the chip data to outside entities by exploiting the timing channel resulting from inter arrival times of the legitimate transmitted packets. The first design of spyware integrated within the communication circuitry of wireless CSMA/CA that exploits the timing channel resulting from inter arrival times of packets to leak data from the chip. We introduce a covert channel encoding that utilizes the coding methodology developed. This methodology allows us to encode timing information in presence of the worst nonnegative additive noise, the exponential noise.

Our spyware employs a low-complexity error-correcting code framework that is robust to timing perturbations resulting from the CSMA/CA's collision avoidance back-off strategy. This back-off strategy introduces a nonstandard queuing noisy channel that interferes with timing-based communication purposes. We show the difficulty of the spyware detection, both at the hardware level and at the packet timing level, from both theoretical and practical perspectives. To substantiate our theoretical findings and to evaluate the overhead, the spyware is implemented and tested on the widely used WARP wireless radio platform.

V. SYSTEM DESIGN

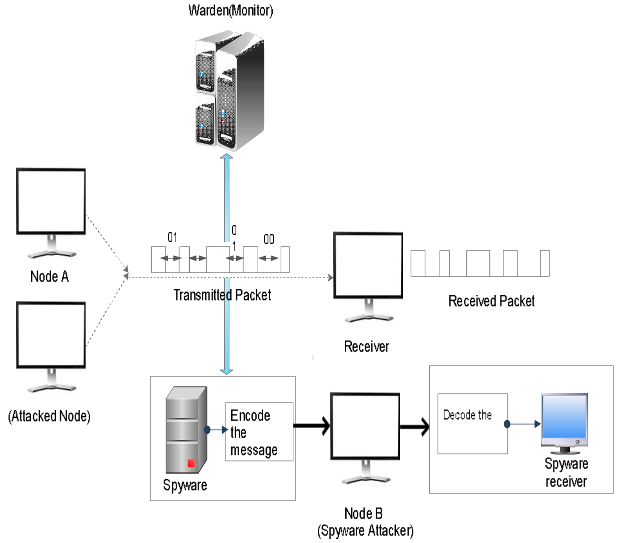

Fig.1.Covertcommunication

From Fig.1: Covert channels are mechanisms for communicating information in ways that are difficult to detect. Packet networks are designed with the goal of communicating through packet content sand their headers and not the timings. Hence, the timing channel induced by the interpacket timings provides aside channel that can be utilized for covert communications. Fig.1 illustrates a covert timing channel between an infected transmitter and a legitimate receiver. The warden sees the exchange of packets but fail store alize the covert communication in packet timings. On the other hand, the spyware receiver, which has side information pertaining to the parameters of the encoding scheme, it can decode the message conveyed through timings.

VI. IMPLEMENTATION

a. Triggering the spyware

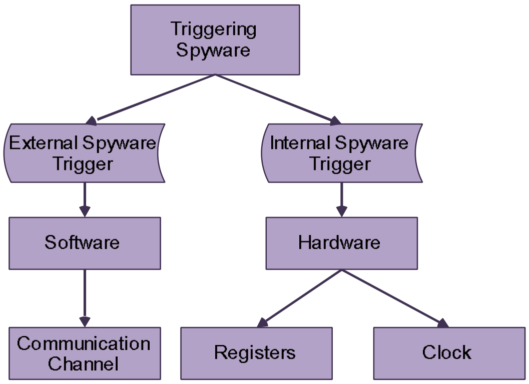

Fig.2-Triggering the spyware

The spyware is activated upon the arrival of a trigger, which may come from either internal or external sources. The spyware does not need to be active all the time. We call the active duration of a spyware the spying interval. An internal spyware trigger comes from within the hardware. The two most obvious choices for an internal incitement are the states of the registers in the design, and the clock. The states of the register can be utilized in a number of ways—for example, by arriving at a certain internal state of the communication controller, or upon reaching a certain counter state.

b. Spyware process

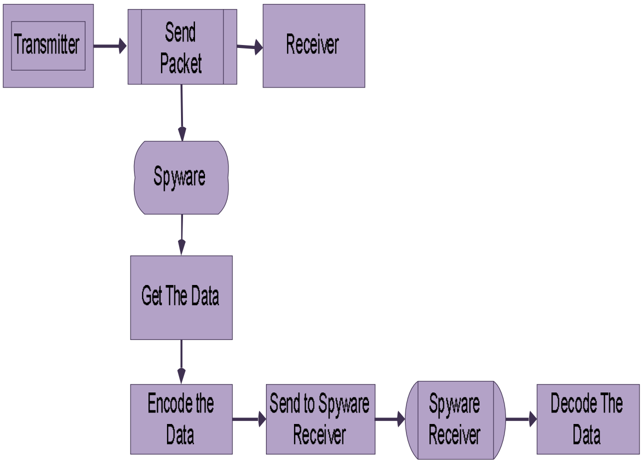

Fig.3-Spyware process

Covert channels are mechanisms for communicating information in ways that are difficult to detect. Packet networks are designed with the goal of communicating through packet contents and their headers and not the timings. Hence, the timing channel induced by the inter packet timings provides a side channel that can be utilized for covert communications. A covert timing channel is between an infected transmitter and a legitimate receiver. The warden (aka eavesdropper) sees the exchange of packets but fails to realize the covert communication in packet timings. On the other hand, the spyware receiver, which has side information pertaining to the parameters of the encoding scheme, can decode the message conveyed through timings. The CSMA/CA protocol results in random delays in the packet inter arrival times. We will model the impact of the CSMA/CA as a first-come first-served (FCFS) queuing system.

c. Warden monitoring process

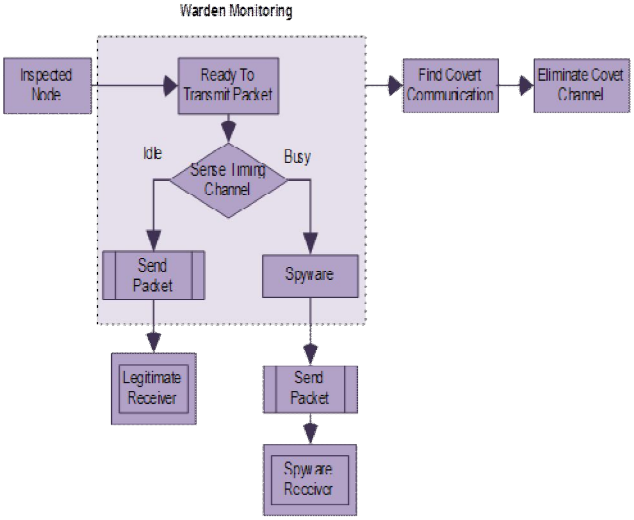

Fig.4-Warden monitoring process

The counter measures to covert timing channels come mainly in two flavors: detection and disruption. The detection of covert timing channels is based on statistical tests that can distinguish between legitimate and covert traffic. The disruption (e.g., jamming) of covert timing channels is done by an active warden that aims at preventing the covert communication usually with the undesired side effect of degraded system performance. While the countermeasures to covert timing channels come mainly in two flavors: detection and disruption. The detection of covert timing channels is based on statistical tests that can distinguish between legitimate and covert traffic. The disruption (e.g., jamming) of covert timing channels is done by an active warden that aims at preventing the covert communication usually with the undesired side effect of degraded system performance.

d. Warden table:

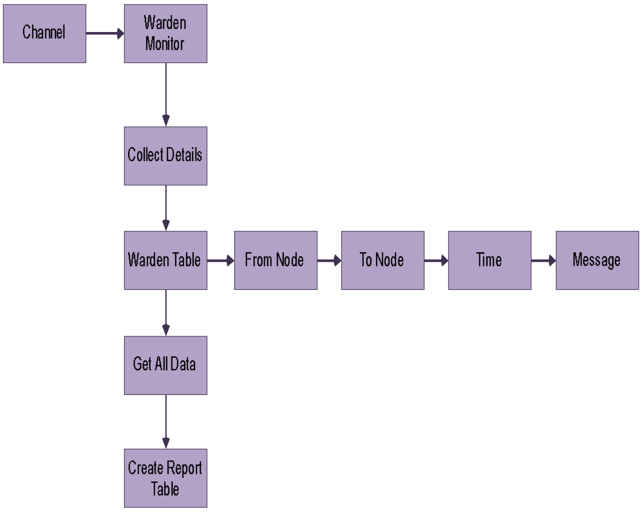

Fig.5-Warden table

Warden continuously monitor the channel and collect all information. Then create a report table .The report details are sender node, receiver node, transmit time, packet Name. Get all details then find the report table. The report table used to find the spyware.

e. Detection of spyware:

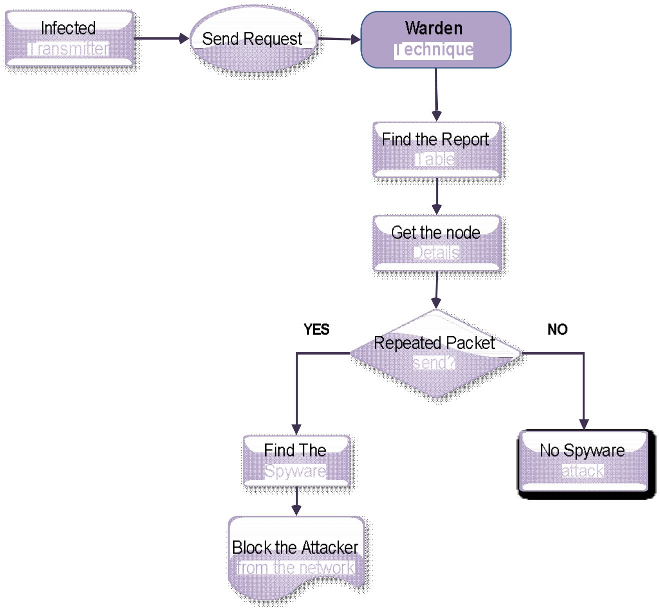

Fig.6-Detection of spyware

Other special purpose detection tests that are designed for specific covert timing channels include similarity for IP covert timing channels and mean–max ratio to test for binary or multi symbol covert timing channels. The mean–max ratio test assumes that the legitimate inter packet delays follow a normal distribution which is often not true for real network traffic. That none of the above tests can reliably detect the presence of covert communication.

VII. DATAFLOW DIAGRAM

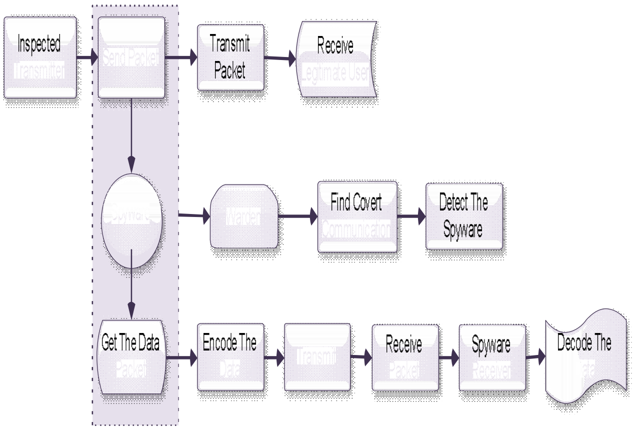

Fig.7-warden techniques

The spyware affected system is an inspected transmitter; this transmitter is used to send the packet. While sending the packet it sends to the legitimate user and the spyware initiator also. The spyware is used to get the data packet and encode the data then transmit the packet to the spyware receiver which is used to decode the data. At the same time it is used to store in the warden techniques which is help us to find covert communication and then it will detect the spyware and identify the spyware initiator.

VIII. PERFORMANCE AND EVALUATION

FROM	TO	PACKET	TIMING
NODE	NODE	NAME	
A	B	Connection.java	19:20
A	C	Connection.java	19.21
A	B	Normal.java	10.22
A	C	Normal.java	10.23

It consists of FROM NODE, TO NODE, PACKET NAME and TIMING. The sender addresses are stored in from node. The receiver addresses are stored in To node. If the node A send a message to node B, then the same message send to the spyware activator. Our proposed work, focus not only in detecting the spyware initiator but also identifying the initiator. By using the warden techniques we easily identify the spyware initiator. A single Node can attack by single spyware initiator.

Graphical Representation:

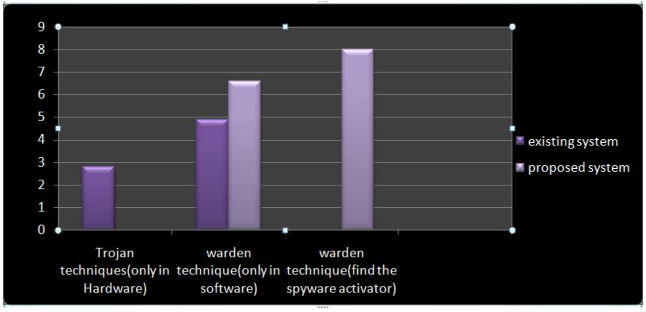

Fig.8-Performance and evaluation

It shows the performance evaluation of the existing and proposed system. In Existing system, spyware detect in hardware and software not finds the spyware initiator. In proposed system we find the spyware initiator using timing channel.

IX. CONCLUSTION

A new methodology for the design and implementation of spyware communication circuits that exploits the CSMA/CA MAC protocol properties to covertly leak the chip data to an intended spyware receiver. Our proposed scheme is robust to the collision avoidance techniques in the CSMA/CA protocol of the MAC layer. We interweave the encoder in the states and transitions of the wireless transmitter presynthesis, such that distinction and uncoupling of the spyware from the radio's physical layer is impossible. The spying act is initiated upon an occasional external or internal trigger. The proof-of-concept implementation is demonstrated on the widely used Wireless Open Access Research Platform (WARP). Three metrics were used for evaluation of the spyware performance: 1) efficiency of the encoder implementation, which was theoretically demonstrated; 2) robustness of the communication method to CSMA/CA effects, which was done by simulating the wireless architecture across a range of parameters; 3) difficulty of covert channel detection that was shown to be resilient against the known covert timing channels detection methodologies. While there exists a trade-off between accuracy, overhead and detect ability, our experimental results show that our implemented spyware simultaneously meets the desired above metrics.

X. FUTURE WORK

In our proposed design we not only detect the malware but also indentified the intruders who install the malware program in our system. Making use of warden technique we identified. In Future, by using time delay we expect to identify the malware as early when it hit our system. And also, by using network auditing technique we can identify the malware at the time of installation.

REFERENCES

[1] Li Yang et al: "Real-Time Detection of Covert Channels in Highly Virtualized Environments" may.2011
[2] Negar Kiyavash et al :"A Timing Channel Spyware for the CSMA/CA Protocol"jan.2013.
[3] Y. Jin and Y. Makris, "Hardware Trojans in wireless cryptographic ICs," IEEE Design Test Comput., vol. 27, no. 1, pp. 26–35, Jan./Feb. 2010.
[4] S. Adee, The Hunt for the Kill Switch May 2008 [Online]. Available: http://www.spectrum.ieee.org/may0
[5] S. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou,"Designing and implementing malicious hardware," in Proc. USENIX 2007.