Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 3, March 2018, pg.25 – 32

Survey based on Cyber Attacks in Closed Loop Control Systems

R.B.Benisha[1], S.Raja Ratna[2]
[1]Department of CSE & V V college of Engineering, Anna University, India
[2]Department of CSE & V V college of Engineering, Anna University, India
[1] beni.rb53@gmail.com; [2] gracelinrr@yahoo.com

Abstract— In this paper, attacks caused in the shut circle control system is discussed. To keep the net-worked control systems safe, good, ready and hard to move, getting NCS from of the net attacks is very important. The marked power of thought attackers will not move after any made suggestion copies made to scale, they keep on changing their attack designs as if by chance and dynamically. Distributed go into discovery system (DIDS) is used to discover the of the net attacks in the shut circle control system. The end of this paper is to over-view different types of attacks that are taking place in the shut circle control systems. Different expert ways of art and so on, questions, discovery, putting a stop to of the net attacks in the control systems are high-lighted.

Keywords— Cyber attacks, cyber physical Systems, Wireless automation, secure control systems, DIDS, Networked control systems (NCS)

I. INTRODUCTION

Wireless networks are made distributed, infrastructure-less, fault -tolerant, scalable and forceful in nature [1]. Radio networks are open to attack to different types of attacks and safety being, saying violent behaviour that can make waste the doing a play of the networks [1]. They try to keep safe the network safety secretly, network safety true, good nature and network safety able to use. Several types of attacks come to mind in the shut circle control system. More specially, in the existence of an undesired one going in (or attacker), the parts and the gave news to knowledge in the control system are thing talked of to hearing private talk on purpose and taking care of expertly which can act on its without change, stable and doing a play and leads to system degradation.

Denial of service, Replay attacks, Integrity attacks are the conman attacks that are occurring in the closed loop control system. A closed loop control system has one or more feedback loops or forward paths between its input and output. So that if any malicious attacks occurs in the closed loop control systems, error occurred can be identified through the feedback loops [2]. Networked control system uses the concept of

Wireless control systems in which the design and the topology consists of plant, controller and the intermediate network. Attacker influences the communication channels in the control system.

System (DIDS) is used to discover the of the net attacks that gives lower, less important position to the doing a play of the shut circle control system. A made distribution IDS (dIDS) is chiefly of number times another go into discovery systems (IDS) over a greatly sized network , all of which exchange with each other, or with an in the middle of computer that helps increased network looking at, small event observations, and short time attack facts. go into discovery system (IDS) is a safety apparatus used to discover the not normal behaviour in the network. In order to increase the being strong and safe the control systems right apparatus for making or put right things should be used to put a stop to from different types of attacks [3].

This paper summarizes the concept as follows: Section II describes the analysis of attacks. Section III describes the Intrusion detection methods used to detect the attacks, section IV describes the literature survey and V describes the problems in current detection attacks and VI concludes the paper.

II. ATTACK ANALYSIS

The radio net-worked shut circle control system, there is an important existence without of safety methods which has existence a new opening, nothing in between the ones that makes of the safety technology and the ones that makes of networks. A computer expert for pleasure will be hearing private talk on purpose the news channel, get the facts and make different the note and pump in false day send word through the channel. In the net-worked control systems several attacks are occurred because of, in relation to unawareness in the radio net-worked system. No trust in public organization attacks, Replay attacks, stealthy attacks, deception attacks, false facts pumping in attacks, Bias pumping in attacks etc. These attacks may get broken up the facts and causes degradation in the system operation and cause profit loss.

An attack may be an action-bound or action-less attack [2]. In action-bound attack, the attacker will undergo some actions which may change the system resources like breaking or going round the got systems, mostly it results in letting be seen sensitive knowledge, adjustment of facts or the greatest, and loss of knowledge for computers completely. Trojan horses, a cause of diseases, worms, putting in bad code 1, getting into network facts, going out quietly login news given are some of the examples for the in operation attack[4][5]. This sort of attack is very damaging to the system. The types of in operation attacks are: take the part of, meetings play again, adjustment of note.

An action-less attack tries to have knowledge of or to use some important knowledge but it does not act on the system use-able things. In this sort of attack, the attacker uses some sniffer apparatus for making or put right things coming through slowly the let-through secret words are some of the action-less attacks [6]. The types of action-less attacks are: give out note of what is in and business trade observations.

A. *Denial of Service Attacks*

In this attack, a block in a given authority user's way in to a knowledge processing machine network, representatively caused with bad intent. The bad net-work point will get moved from one position to another and gets used up bandwidth of the complete network. The main purpose of this attack is to make the network hard growth and having much to do by getting in the way of the notes being transmitted. If any note comes from an unauthenticated person the network will not give a reaction to the person since it is busy [7]. The DoS attack comes to mind to do with industry control systems, SCADA systems, linear systems, Multi-agent systems and so on**.**

B.Stealthy Attacks

A careful moving attack could be formed by an action-bound person who questions knowledge for computers small parcels from and to your network so in connection with discover a careful way to middle way the safety. Once the safety is put at risk or in other words, once the computer expert for pleasure gets way in to your network, the user puts to use it for a short stage of time for his gains and then, takes away all signs of the network being put at risk[2][8]. The focus, it seems in this Case, is on taking away the signs of attack so that it remains unmeasured for long. In this attacks zero driving power attacks are occurred commonly in which the attackers keep being in working state. The methods used in the moving carefully methods are evasion, targeting dormancy, determination, complex. To make certain your safety system has in it elements that can digital copy root kits for malware. As they amount before your safety system, they unnatural position a good sign of danger. In addition, since they are at rest until the time is ready for an attack, they are hard to discover. A good amount of network business trade-off observations is needed for getting together facts over a time and then checking for making connections to unknown or unwanted addresses can help counter/prevent careful moving attacks to a good amount.

C.Replay Attacks

In play again attacks, it captures the interactions that are sent by the user through the wireless network and the information will released or retransmitted after a long time after its processing has been over. This type of attack is also called Man-in-the-Middle attack. The eavesdropper will use till its process has been changed, after completion it will send the information after a long time. During this delayed process the intruder will hack the information. This attack can be prevented by analyzing and encrypting the identity to each of the component. So that they are not independent on each others, if the attacker enters the network. Attacker cannot replay since they have different ID. Due to play again attacks time delay, more energy is consumed.

D.Deception Attacks

Deception technologies products can discover, get at the details of, and put forward arguments for against zero-day and increased attacks, often in true time [9]. They are made automatic, accurate, and make ready knowledge into bad operation within inside networks which may be unseen by other types of the net making attempt to keep from attack [11]. Deception technology enables a more before-the-fact safety position by looking for to trick the attackers, discover them and then over-come them, letting the undertaking to come back to normal operations. A deception attack most commonly comes to mind in the SCADA systems. Deception technology is put forward to give greater value to rather than put in place of the other safety products an organization uses. Deception attacks can make vulnerabilities when the input values are changed by a hacker. The user does not know the unusual changes in the controller when the system is in use.

E.False Injection Attacks

False pumping in attacks have relation to a wide part of attack gives directions to be taken that let an attacker to supply untreated input to a program, which gets processed by an one who makes clear from a different language as part of a need or question which makes a change in the direction of Execution of that program [13]. These pumping in attacks are among the most old and most dangerous net structure application attacks. They can outcome in facts crime against property, data loss, loss of knowledge for computers true, good nature, words saying not true of arm, as well as full system compromise. False facts pumping in will occurs more frequently in Ac state estimation [15[16].

The first form notes are having stops by the attacker and made different by pumping in the false facts in to it by giving lower, less important position to the system performance. False Injection is a chief hard question in net structure safety. It is listed as the number-one net structure application safety danger in the OWASP. For good reason, pumping in attacks, particularly sql pumping in (SQLi) and Cross-site rough writing xss are not only very dangerous, but they are also very stretched wide, especially in legacy applications. These attacks can be sensed using simulation 6 apparatus for making or put right thing.

F.Bias Injection Attacks

In the tendency in a certain direction pumping in attacks the original knowledge on which reasoning is based are made different and another false knowledge on which reasoning is based are made different and sent through the network. The attacker effects the narrow ways and make different the knowledge which leads to system degradation and cause small parcel loss and system changing state. The force to limit for the attacker is that it wants to keep being unmeasured.

The tendency in a certain direction pumping in attacks keeps safe the nature of left-over distribution, since it remains Gaussian. Since the attack changes the middle, half way between values of the distribution, the danger sign how probable can increase. For this reason, we take to be true that the force to limit the attacker is to considerably increase the danger sign when it is not probably used in the networked control system. Bias Injection attacks use False Detection and Residue problem for detecting the problem of attacks and the residue can be filtered in such types of attacks.

G.Integrity Attacks

Electronic knowledge is uncorrupted and can only be made way in or made different by those given authority to do so. true, good nature has to do with supporting the persons of representative, having no error and believe-able of facts over its complete existence chain. To support true, good nature, facts must not be changed in going across (from place to place) and steps must be taken to make certain that facts can not be changed by a not with authority person or program[17].

Such measures cover implementing user way in controls and account control to put a stop to wrong changes or by-chance being taken out by given authority users. Other measures cover the use of check sums and cryptographic check sums to make certain of true, good nature. network the government measures to make certain facts true, good nature cover documenting system the government ways, parameters and support operations, and making come into existence shocking event got over a disease plans for events such as power outages, computer unsuccessful person or safety attacks. Facts become bad errors or changes, back-ups or Redundancies must be ready (to be used) to put back to earlier position the acted-on facts to its right state and these attacks are occurred mostly in the control systems for the retrieval of data and information so that the total system may lead to financial loss of the whole closed loop control system.

Measures must also be taken to ensure integrity by controlling the physical environment of networked terminals and servers because data consistency, accuracy and trustworthiness can also be threatened by environmental hazards such as heat, dust or electrical problems. Some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse Practices followed to protect data integrity in the physical environment include keeping transmission media (such as cables and connectors) covered and protected to ensure that they cannot be tapped, and protecting hardware and storage media from power surges, electrostatic discharges and magnetism.

III.INTRUSION DETECTION SYSTEM

IDS is the act of sensing actions that attempt to middle way the secretly, true, good nature or able to use of a useable thing. An IDS is an apparatus or software application that guides a network or systems for bad operation or agreement violation. Any sensed operation or breaking is stated either to a controlling person or it will be self control chiefly using a Security knowledge and Event business managers SIEM system. This SIEM trading groups all the out-puts from number times another starting points, and uses danger sign coming through slowly techniques to see what is different bad operation from false danger signals. Though the firewalls 4 and IDS both have a relation with to network safety, a IDS is different from a firewall in that a firewall looks on the outer side for thing being force into in order to stop them from event. Firewall limits way in between networks to put a stop to go into. IDS can be put in order based on where discovery takes place (network or man giving food, room and so on) and the discovery careful way that is employed. They go into system and is able to discover the un wanted twisting and noise by the details as to how things are to be done of the number of times.

Based on Location:

NIDS are placed at a tactical point or points within the network to computer viewing output the business trade on the network. It does observations of going past, through business trade on the complete subnet and matches the business trade which is passed on the subnets to the group of experienced attacks. If an attack is taken or any not normal behavior is sensed, the ready can be sent to the controlling person. Example. Loud noise through the nose.

Host intrusion detection systems:

HIDS work on one only animal on which another is living on the network. This HIDS computer looking-glass inbound and outbound small parcels from the apparatus and will ready the user or controlling person if any doubtful operation is discovered. It takes a copy of having existence system records and matches it to the earlier copy. If the full of danger system records were different or taken out, a ready made different or taken out, a ready is sent to the controlling person to make observation off. Example. Ossec aide. based on discovery methods.

Signature-based detection system:

Signature-based IDS says something about to the discovery of attacks by looking for special designs like byte orders in network business trade or some well experienced bad teaching orders used by the attacker. Although signature-based IDS can easily discover experienced attacks, it is not possible to discover new sort of attacks because there is no good example kept ready (to be used). But, the sign of danger of network go into much wider than those heavily made public small events of net structure place defacement. In material fact, the sign of danger of network go into hangs over any organization that is owner of a network that is open to the outside earth.

Anomaly-based detection system:

Anomaly-based IDS are particularly introduced to discover unknown attacks, and able to do up with the quick development of malware. The basic idea is to use machine learning to make come into existence a design to be copied of safe operation and then make a comparison of new behavior against this design to be copied. Although this way enables the discovery of new sort of attacks, it have pain, troubles from false positives which is also a bad operation, particularly introduced to discover unknown attacks, to (be able to) do up with the quick development of malware. The basic idea is to use machine learning to make come into existence a design to be copied of safe operation and then make a comparison new behavior against this design to be copied. Although this way in enables the discovery of new sort of attacks, it have pain, troubles from false positives which is also a bad operation

IV. LITERATURE SURVEY

The work-place on different IDS techniques suggested by different Authors, the being like net structure attacks and the way it can be sensed is presented here. The reasoned opinion that can be outlined from the above made into one take views of go to person in authority is, the papers [10] to [13], [16] and [18] are designed only to discover one network attack. The techniques involved in these papers are more redundant to its applications. The drawbacks specify the future research. The paper [15] is for attacks namely ddos and animal Force Attack. In [8], it presents a IDS just to get changed to other form a number of not wanted alerts produced by a normal IDS in all types of networks. The authors specified that all attacks caused in the control systems are vulnerable and leads heavy damage, system loss and financial crisis. They introduced adapted algorithms to detect and solve such types of attacks. The different techniques used for the discovery of attacks are described and given under:

Technique	Description	Advantages	Disadvantages
Sub component normalized with SNORT IDS[2]	Reduction of large number of alerts from IDS	Reduce unimportant alerts, produces better results	High false alarm rate and system to lower false alarm rate is needed
TOPASE [3]	DDOS attack	Effective in terms of dropping and wasting	Need caution in setting optimal thresholds
Fitness function of genetic algorithm [5]	Integrity attacks	Enables dynamic and adaptive redirection of traffic	Needs mechanism to prove cloud-based IDS, performance
IDS using open flow [6]	Network attack	Provide a secured platform for sharing	System is not designed for encrypted data sharing

SQLiDDS and intrusion detection system[8]	SQL injection attack	Overall accuracy is high and false positive rate is low	Algorithm provides less number of high quality clusters
Wamid and anamoly based detection [9]	SQL injection attack	Provides double layer security to the system	Extended to include detection against attacks
Approach with white list approach [10]	SCADA systems with DDos attack	Combines multiple models and detects most of the data that are attacked	Lack of information leads to redundant hypothesis

V. PROBLEMS IN ATTACK DETECTION

Attack discovery are based on much knowledge of signatures of experienced attacks looked at events are matched against the signatures to discover attacks. These methods get out features from different looking over of accounts by expert stretches out, and discover attack by making a comparison the point values to a group of attack signatures on condition that by to do with man experts. The sign-mark knowledge-base has to be done with the hands gone over for each new sort of attacks that is discovered. If the network is small and signatures are kept up to day, they do with man and observer answer to attack discovery works well. But when organizations have a greatly sized, complex network they with man observers and quickly become over-came according to the rules of danger signals they need to have a look into. The old and wise design to be copied of discovery has put up inefficient and the price of make observations is so much. in addition, with more and more facts becoming ready (to be used) in by numbers, electronic form and size and more applications being undergone growth to way in facts. The facts and applications are also one attacked person of attackers who great act these applications to profit way in to facts. With the placing of more simple safety apparatus for making or put right things and to keep safe (out of danger) the facts and arms, the attackers often come up with newer and more increased methods to over-come to put in safety systems. An important limiting condition of having existence go into discovery methods is that they can not discover violent behavior, since their very nature, saying violent behavior are pushed into water using previously unknown attacks. In addition, even if a new attack is discovered and its sign-mark got greater, stronger, more complete, often there is a with substance latency in placing across networks. These limiting conditions represent the hard question with the currently having existence attack discovery system, and have led to an increasing interest in attack discovery expert ways of art and so on.

VI. CONCLUSIONS

This paper presents some basics of the net attack discovery system with the details of safety name-giving tickets in a shut circle control system. in addition, the questions and requirements for very small grains attack discovery system with the problems in current attack moves near are also had a discussion about, which may help the person by making observations to better get through knowledge in the attack discovery system. The presented shortcoming of current safety moves near may help the persons in making observations and building a safer network safety system.

REFERENCES

[1] *Overview of Attack Trends*, Last accessed: November 30, 2015. http://www. cert.org/archive/pdf/attack_trends.pdf.

[2] Kapil Kumar Gupta, Baikunth Nath, Kotagiri Ramamohanarao, and Ashraf Kazi. *Attacking Confidentiality: An Agent Based Approach*. In Proceedings of IEEE International Conference on Intelligence and Security Informatics, pages 285–296. Lecture Notes in Computer Science, Springer Verlag, Vol (3975), 2016.

[3] Jian Pei Shambhu J. Upadhyaya Faisal Farooq Venugopal Govindaraju. Proceedings of the 20th International Conference on Data Engineering (ICDE"04) 1063-6382/04 $ 20.00 © 2004 IEEE [4] Debar, H., Dacier, M., and Wespi, A., *A Revised taxonomyfor intrusion detection systems, Annales des Telecommunications*, Vol. 55, No. 7–8, 361–378, 2014.

[5] Jackson, T., Levine, J., Grizzard, J., Owen, and H., "*An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network*," IEEE workshop on Information Assurance and Security, IEEE, 2017.

[6] D. Y. Yeung, and Y. X. Ding, "*Host-based intrusion detection using dynamic and static behavioral models," Pattern Recognition*, 36, 2016, pp. 229-243.

[7] X. Xu, and T. Xie, "*A reinforcement learning approach for host-based intrusion detection using sequences of system calls*," In Proc. of International Conference on Intelligent Computing, Lecture Notes in Computer Science, LNCS 3644, 2014, pp. 995-1003.

[8] Krasser, S., Grizzard, J., Owen, H., and Levine. J., "*The use of honeynets to increase computer network security and user awareness*," Journal of Security Education, vol. 1, 2014, pp. 23-37.

[9] Shon T., Seo J., and Moon J., "*SVM approach with a genetic algorithm for network intrusion detection*," in Proc. of 20th International Symposium on Computer and Information Sciences (ISCIS 2013), Berlin: SpringerVerlag, 2005, pp. 224-233.

[10]X. Xu, X.N. Wang, "*Adaptive network intrusion detection method based on PCA and support vector machines*," Lecture Notes in Artificial Intelligence (ADMA 2013), LNAI 3584, 2005, pp. 696-703.

[11]Asmaa Shaker Ashoor, Prof. Sharad Gore —*Importance of Intrusion Detection System (IDS)*‖ International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January-2017

[12]Marchette, D., *A statistical method for profiling network traffic,* First {USENIX} Workshop on Intrusion Detection and Network Monitoring, Santa Clara, CA, 2014, pp. 119–128.

[13]McCanne, S., Leres, C., and Jacobson, V., libcap, available via anonymous ftp at ftp:// ftp.ee.lbl.gov/, 2014.

[14]James P. Anderson, "*Computer security threat monitoring and surveillance,*" Technical Report 98-17, James P. Anderson Co., Fort Washington, Pennsylvania, USA, April 2012.

[15]Dorothy E. Denning, and P.G. Neumann "Requirement and model for IDES- *A real-time intrusion detection system*," Computer Science Laboratory, SRI International, Menlo Park, CA 94025-3493, Technical Report # 83F83-01-00, 2016.

[16]H. S. Javitz and A. Valdes. *The SRI IDES Statistical Anomaly Detector*. In Proceedings of the IEEE Symposium on Security and Privacy, pages 316–326. IEEE, 2017.

[17]Barbarà, D., Couto, J., Jajodia, S., Popyack, L., and Wu, N., ADAM: *A Testbed for Exploring the Use of Data Mining in Intrusion Detection,* ACM SIGMOD Record, 30(4), 2001,pp. 15-24.