International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

SCADA Systems: Vulnerabilities and Blockchain Technology

Diksha Chhonkar, Garima Pandey

Student, Department of CSE, Dronacharya College of Engineering, Gurgaon, Haryana, India

ABSTRACT

SCADA systems are one of the most important part of industrial operations. Before SCADA, plant personnel had to monitor and control industrial process via selector switches, pushbuttons and dials for analog signals. As manufacturing grew and sites became more remote, relays and timers were used to assist supervision. With the onset of technology and advent of network based protocols, these systems became more reliable, fast and it became easy to troubleshoot problems. Indeed progress also brings vulnerabilities, which was no new for SCADA. The IP protocols brought threat to the security of these systems. The devastation that cyber predators on SCADA can inflict, could be illustrated by the Stuxnet virus attack. This paper discusses what SCADA systems are, their uses, protocols being used by these systems, vulnerabilities and ways to combat those vulnerabilities. It focusses on the use of Blockchain Technology as a step in security of such systems.

KEYWORDS: *SCADA systems, Vulnerabilities, blockchain technology, decentralization*

How to cite this paper: Diksha Chhonkar | Garima Pandey "SCADA Systems: Vulnerabilities and Blockchain Technology" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.1548-1550, URL: www.ijtsrd.com/papers/ijtsrd31586.pdf

IJTSRD31586

Introduction to SCADA Systems:

SCADA stands for Supervisory Control and Data Acquisition. It is a collection of both software and hardware components that allow supervision and control of production plants, both locally and remotely and is used to gather real time data. It consists of HMIs (Human Machine interaction) which facilitates interaction with field devices such as pumps, valves, motors, sensors etc. SCADA software usually links the databases and HMIs. The structural design of a standard SCADA system starts with RTUs (Remote terminal Units) or PLCs (Programmable Logic Controllers). RTUs and PLCs are microprocessors which communicate with field devices and HMIs. The data from RTUs and PLCs is then routed to SCADA computers where software interprets and displays the data to operators for analysing and reacting to system events. Before SCADA, monitoring and control was the task of plant personnel. In 1960s, with the growth of manufacturing, telemetry came on the scene to offer automated communication. In 1970s, the term SCADA was coined for standalone units with PLCS and microprocessors without networking. Later in 1990's and 2000's SCADA system started to implement open system architectures with communication protocols allowing real time plant information to be accessed anywhere around the world.
With SQL, data history can be logged and used in trending applications and record keeping. On HMI and end user computer, graphical representation of operations exist for operator interactions. Data may be analysed and used to enhance plant production and troubleshoot problems.

Uses of SCADA Systems:

The sesystems are used in industrial organisations such as Oil and Gas refining and transportation, telecommunication, water and waste control etc. as they help in maintaining efficiency, processing data for smarter action. SCADA systems are used for generation, distribution and transmission of electric power enabling detection of current flow and line voltage. These systems are successfully used by manufacturing units for regulation of industrial automation, for monitoring the process and controlling the quality of it. SCADA is also used to automate, monitor and control all the function related to railway trains and trolleybuses. Waste water and sewage utilities use these systems to monitor and control the water pump station. SCADA is also used by offices and building environments, thermal station and power plants and industries like forestry, pulp and paper industries.

Protocols used in SCADA Systems:

Protocols allow SCADA/ RTU units to communicate with each other. Protocol and communication parameters should match between connecting devices. There are more than 200 such application layer protocols like Modbus, Allen Bradley DF1, Omron, Siemens and Mitsubishi etc. These protocols are now used as virtual standards in modern SCADA systems. Modbus is a communication protocol given by Modicon Systems in 1979 used for transmitting information over serial lines between electronic devices. Three main variations of Modbus protocol include Modbus ASCII, Modbus RTU and Modbus TCP. Distributed Network protocol (DNP) is a member restricted protocol. It has gone through various iterations. Modbus X is an adoption which overcomes the Modbus limitations by allowing positive and negative numbers up to 9 digits making it legible. Ethernet is

a packet oriented protocol. The packets are generated irrespective of the incoming data protocols. TCP/IP networks have the same packet characteristics as Ethernet and frame relay network. It must establish connection before transferring data as it is connection oriented. Once the connection is established, the server then responds to the queries from the client until the client closes the connection.

Vulnerabilities of a SCADA System:

Many Vulnerabilities can pose as a threat for such systems like hackers, security-unaware employees, Malware, Lack of Software and Hardware maintenance. Critical infrastructure threats include equipment failure, terrorist attacks, accidents, crimes and natural disasters. These may be reasons for failure of such systems. Hence these systems need to be made robust and should be maintained on a timely basis. Apart from Hardware loses and attacks, the more vulnerable part is the software as the hackers and other cyber predators are one step ahead. According to a risk report, around 60 % of such sites aren't using anti-virus protections throwing a risk of updating signatures automatically. Around 70% sites use easily crack able passwords which could lead to denial of service, manipulation and data interception.

There may be hackers who gain access to the SCADA network may make some unauthorized changes to instructions and commands by compromising the servers. This could be an act of outsider or insider where different information to operators and control systems could be presented. Majority of SCADA network have Master Stations which can control the systems and if these stations are not protected by firewalls, antivirus or other methods can lead to undesirable conditions. Equipment protection systems could be messed up and can lead to destruction in costly and irreplaceable equipment. Interference in safety system canal so endanger human life.

Combating SCADA Vulnerabilities:

With the usage of client–server based protocols, the problem of security of the network is encountered. The prominent challenge is to restrict the unauthorized access. Then comes the question of enhancing security inside the SCADA network and to develop security monitoring tools. Focus should also be diverted to cryptography and key management along with the device and operating system security management. There is very little emphasis on standard security methods like encryption and authentication. A robust protection strategy is the need of the hour for such systems. It is high time to realize the importance of implementing security programs. Some strategic steps may include removing of unnecessary functionalities and mapping of current systems and knowing all points of entry and exit which pose as threats are much easier to monitor. Secondly, early detection of potential attacks can limit the amount of damage done. Constant security checks and risk assessments should be conducted timely. Many techniques like encryption and firewalls can protect such systems. Clever techniques like "honeypots" can deal in some manner to counteract unauthorized access attempts. As many SCADA Systems use master control systems which become an easy prey for the cyber predators to attack. These systems can also be decentralized and made more reliable and safe.

Blockchain: A solution for cyber threats

One way to make SCADA secure is by making t h e s y s t e m decentralised because decentralisation will reduce dependence on a particular master station for controlling and monitoring operations. Blockchain is a distributed database which maintains records of all device transactions data on a SCADA blockchain network. Basically, blockchain comprises of two words where block means digital information and chain means storage in public database. The blocks have three main parts of information that is information about transaction for example duration and amount of purchase from any e-commerce site. Secondly, it contains information about end user who is participating in transaction and also the information to differentiate it from other blocks. The data is stored in blocks forming a linear sequence where each block references the hash of the previous block. A hash is a unique ID of a block. Anybody who tries to temper with the hash needs to change all the hashes of successive blocks which makes it a tedious task and therefore the data becomes temper proof. The working of this technology combines three leading technologies that are cryptographic keys which could be private as well as public, a peer-to-peer network containing a shared ledger and a machine which is used to store transaction and records of the network. The cryptographic keys produce a secure digital reference and play an important role in successful transaction between two parties removing the need for third party. This secure identity is called digital signature in case of crypto currency. The digital signature is combined with peer-to-peer network where large amount of individuals act as authors and transactions are carried out efficiently. Advantage of the Blockchain is the greater throughput of the database technology, faster data Communication technology, efficient consensus mechanism to make sure the security of SCADA. These transactions data are time stamped and can be checked whether the sender's data and the receiver's is validated. Also blockchain use efficient consensus mechanisms and algorithms which ensures that legitimate transactions are added and synchronizes and audits them. These consensus protocols are necessary for correct functioning of blockchains. Some of these mechanisms are Proof of Work (POW), Proof of stake (POS), Proof of capacity (POC) and Proof of Elapsed Time (POET) etc. POW is also known as mining and requires solving of complex and asymmetric mathematical puzzles. These puzzles are solved on a hit and trial basis and depends upon good computational power. The difficulty of the puzzles depends upon how fast the blocks are mined. POS is a randomized process in which producer of next block is determined. This method is energy efficient and validators actually maintain the network as they hold the coins of blockchain they are validating on. In a delegated proof of stake method users can vote for a particular delegate. A person or organisation that wishes to add blocks to a network refers to a delegate. This method is also called digital democracy. POC is another method which uses plotting whoever having the fastest solution of puzzle creates a new block. POET is a protocol in which assignment of random wait time to each node is done. Hence blockchain has very crucial features like transparency, encryption and accountability. This means that no single node or group of nodes can take up majority of the set and no one can change entire SCADA network software system without the majority of the entire network of users accepting the change, thus ensuring no harm to the system.

Conclusion:

Use of network protocols in SCADA systems make them vulnerable to cyber attacks. Hence a robust protection strategy is the need of the hour. Blockchain technology being a distributed, encrypted and secure mechanism can be used to ensure security of the system. As blockchain use consensus mechanism to add new transactions, it would not be easy for attackers to change data and present wrong logs thus reducing risks of scada systems.

References:

[1] John D. McDonald and Mini S. Thomas: Power System SCADA and Smart Grids, 2015.

[2] Ronald L Krutz: Securing SCADA systems, 2005.

[3] http://www.bayshorenetworks.com

[4] Daniel Drescher: Blockchain Basics: A Non-Technical Introduction in 25 Steps, 2017.

[5] www.hackernoon.com