An Effective Scheme against Insider Attack

Ru Hui Chua
School of Electrical and Electronics Engineering
Nanyang Technological University
Singapore
E-mail: rchua006@e.ntu.edu.sg

***Abstract*—The supervisory control and data acquisition (SCADA) system is used in both government and private sector worldwide for monitoring and controlling purposes. Considering the advancement of technology in today's world, however, the concern on the possible attacks to such system has raised. While organisations have traditionally placed more focus on the protection against outsider attacks, the detrimental effect caused by the insider attacks has often been overlooked. With the knowledge from the "insider" perspective, it would be easier for an insider to conduct an internal attack and leads to more devastating consequences. Thus, this paper aims to provide an effective scheme for the urban transportation system, which adopted the SCADA system, to protect against insider attack by using a network configuration management (NCM) to manage real time data. In our scheme, RANCID is chosen to be the NCM used to manage devices because it is simpler to install and configure in a Linux environment. Ubuntu is installed in a Linux virtual machine, VMware Workstation 12 player. For network topology simulation wise, Graphic Network Simulation 3 (GNS3) is used to provide a platform to simulate real life network connection for testing and troubleshooting. Our scheme provides the configuration report of the devices in SCADA system that could be accessed by the operators. Devices information is uploaded to web browser by using subversion (SVN) and web subversion (webSVN) in Ubuntu for the operators to keep track on. In this way, our scheme can ensure the safety of each of the devices by checking data uploaded from them. If any of the data provided from device is not as expected, the operator will know that an unauthorized modification has been made and hence proceed to any necessary action to prevent any damages caused to the system.**

Keywords—SCADA; insider attack; RANCID; subversion

I. INTRODUCTION

Due to the advancement in technology over the recent years, technology has become the most important thing that drives human daily routine in all different walks of life. However, intruders with various reasons and motivations have been trying or had successfully hacked into various organizations to infiltrate the system to access confidential information which will jeopardize the whole nation's interest and can sometimes be disasters.

One of the examples of the attack would be terrorist attack into the US military system that stole and leaked the personal information of retired military officers [1]. Although the US department of defence, Pentagon, stressed that there are no more detailed information being hacked and leaked by the group of hackers, the presence uneasiness already successfully caused public panic, especially those retired military officers whose name and address were in the list. If such malicious act is done by an insider of the department, the consequences could be even more damaging as more confidential information might have the risk of being exposed to the public.

Another group of attackers that hacked into various systems and leaked important information is the anonymous group [2]. They broke into various organizations and websites and leaked the users' information or confidential information by claiming that they are doing all this for justice. In 2015, a group of anonymous caused the website of Trump Tower to be down for hours, followed by posting a video online, warning US President Donald Trump to "think twice before he speaks" [3].

The frequency of such attacks has risen in recent few years and it called for public attention and awareness on the security and reliability of the websites, organization system and even their house network. An effective protection scheme against attackers should be the main focus for the entire organization operator as well as public to reduce the risk of being attacked and exposed.

II. SCADA SYSTEM

A. History

Supervisory control and data acquisition (SCADA) system is an industrial control system (ICS) that is widely used in the worldwide nowadays. It is used to keep track of the real-time data besides monitoring and controlling field equipment in each of the organizations and companies. The organizations and companies which adopted SCADA system include oil and gas, food and beverage, packaging, transportation and power industry [3].

The history of SCADA system can be traced back to 1950s and gained popularity from 1960s until now. The usage of SCADA system increases as the need of monitoring and controlling of equipment increases. It was an expensive choice in the beginning since the computer was a costly product. With the rapid development in technologies– where computer has even become a household product -the SCADA system became affordable. The system costs lesser, along with its more advanced improvement in the system technology [4]. Fig.1 shows the SCADA timeline of evolution in the past decades [5].

As it evolves over the last few decades, the performance of a SCADA system has improved vastly. Since many of the organizations using this system are for the crucial services like transportation system and food industry in many countries, the safety and reliability of the system plays a significant role to the organization as well as the public. One of the weaknesses of the SCADA system is that it has a fragile security protection against both external and internal attacks. Hence, the organizations who adopted this system have to work very hard to ensure security of information. However, many organizations and companies had focused mainly on the protection or prevention against external or the outsider attack. For what they did not realize is that the insider attack can also be a thread, that may cause even detrimental consequences than the outside attack, to the organization.

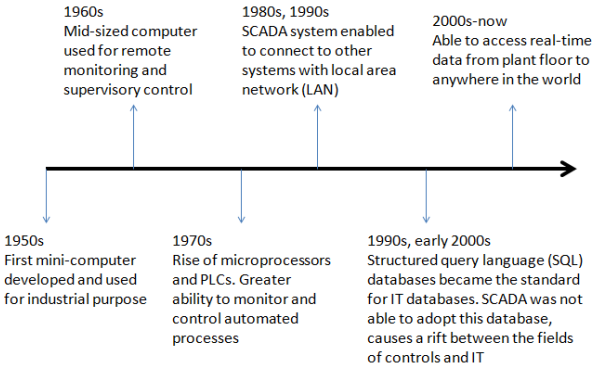

Figure 1. SCADA evolution timeline

B. *Basic Structure*

The subsystems of the SCADA system are the Remote Terminal Unit (RTU), Programmable Logic Controller (PLC), Intelligent Electrical Device (IED) and Human Machine Interface (HMI). It also contains a supervisory system as well as the SCADA programming and communication interface [4]. Each of these is to be discussed below. The basic structure of SCADA system is shown in Fig.2 [6].

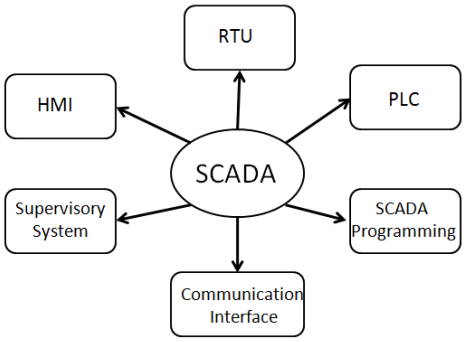

Figure 2. Basic structure of SCADA system

III. Insider and Outsider Attacks

In accordance to Securonix (2015), insider attack occurs less frequent in comparison to the other type of attack to the network by outsider. Therefore, the consequences brought by insider attack are often been overlooked. The damage caused by the insider attack could be deleterious, especially in terms of money. Fig.3 shows the statistics based on the days to resolve the different kinds of attacks and the cost by frequency. It takes more than 54 days to resolve the insider attack and it costs up to $144k per year [9]. Since prevention methods could be taken to avoid such lost, organizations and companies should always look out for a better and more reliable protection against the insider attack.

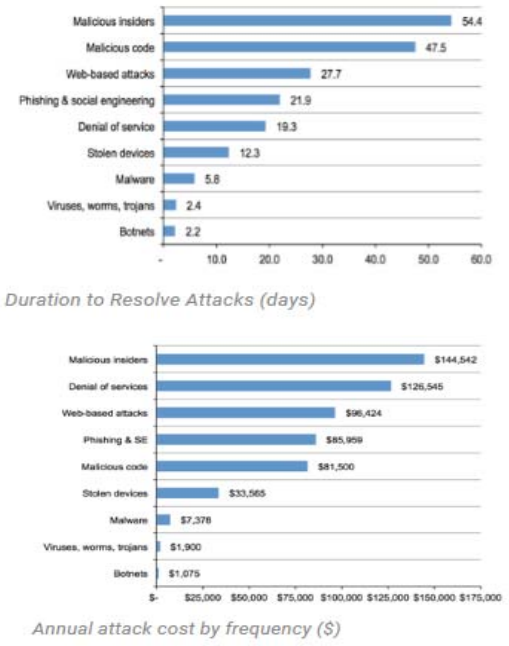

Figure 3. Statistics on duration to resolve attack and annual attack cost by frequency

There are a few categories to differentiate the attackers: attacking from the inside or breaking in from the outside; caused damage on purpose or unintentionally. Fig.4 shows the possibilities of different attackers to the system [3].

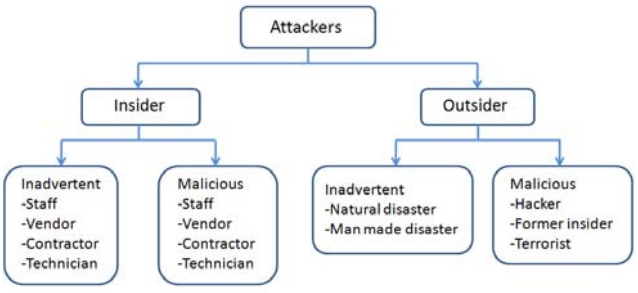

Figure 4. Classification of attackers

A. *Insider*

Usually the insider refers to people with access to the system. The staff with authorized access to each of the different parts of the system, the vendor and contractor who

supplied the system parts to the organization, or even technician hired by the organization for repair or maintenance for the system. These people are more likely to cause higher damage to the SCADA system if they conducted any attack.

With authorized access, staff or technician could carry out malicious attack at the main system itself or the subsystems. They could simply make changes in the setting or the script of the systems to achieve certain result that they wish to see. As they are the key people who are responsible in operating the system, the changes made are usually less suspicious or, in other words, hard to be detected when any damage caused.

Other than the aspects mentioned above, insider attack could also be someone with authority who try to access and attack the system or even someone who get information from the authority person and try to access and attack the system.

However, a staff may make mistakes during his work unintentionally and it may cause damage to the system, and hence it can be considered as an attack to the system as well. This inadvertent attack by insider is harder to prevent as the person might not realize that their action could cause an attack to the system or even already "attacked" the system. Unknowingly attacking the system may ring a faulty alarm to the organization besides requiring more time and resources to recover the system function. Yet, it may also be a good lesson for the organization to raise awareness on such mistakes for the future cases.

B. Outsider

As the name suggested, people who is "outside" of the system is considered an outsider. In other words, anyone without legal or authorized access to the system is what we defined as outsider.

There are different forms of outsider attacks as well. The first form of such attack is inadvertent outsider attack, where is caused by natural disaster or manmade disaster. The attack that caused by the Mother of Natural, for example, earth quake, flood and fire, is hardly prevented but can be prepared on reducing the damage to the least. Sometimes, a careless act by innocent passer-by could easily lead to the damage in the system as well, as simple as spilling water onto the exposed system parts by accident, or damage caused to the subsystem during a car accident. Protection against the inadvertent outsider attack could be done, such as to schedule for regular maintenance to ensure the safety of each part of the systems, or to install water and fire resistant to the system.

The second form of outsider attack is known as the malicious outsider attack. The effect caused by this form of attack could be more serious in all cases. The outsider could be a hacker, a terrorist or sometimes even a former worker of the organization. A hacker may be hacking into an organization system and cause some damage to the system just to prove on his own skills, or to warn the organization for a particular reason. A terrorist could conduct an attack to the organization to cause damage on human life and monetary, and even to steal the confidential information from the government sector or so. For a former worker, who was an ex-insider, might actually conduct and caused the same amount of damage as an insider attack as he was once the authorized personnel to the system. The reason to this is that in most cases, most of the organizations did not clear or remove authorization access of a staff who leaves the company within a short period of time, and hence leave their back door open to the former worker to conduct such attack.

Regardless of insider or outsider, as a malicious attacker, who plans and attacks the organization system must have a very clear and strong purpose that he/she wants to achieve. It may be related to monetary, confidential information, or even human life in some tragic cases. Even though an outsider attack happens more frequently, one should not ignore the power of insider attack. To illustrate the scenario in an example, when someone broke into your house, it would be obvious for you to realize and track the traces left behind to identify any losses or damages done. However, if someone who lives under the same roof has stolen your valuable, it might take you a longer period of time to realize and to find out the way or even the person who did it. The same theory applies in this case. An organization will usually be more alert on any sign of suspicious or unauthorized attempt to its system from the outsider but less aware of the suspicious act carried out from the insider of its own system.

In this paper, we focused on the protection scheme against the insider attack. In order to protect the system, the existing ways are to upgrade the reliability and the safety of the system by implementing software to each part of the system as well as the subsystem. However, as mentioned, insider is the one who has authority access to the system. He may even have the access to the protection layer applied to the system or is able to break it easily. Hence, it is crucial and important to develop an effective scheme that can defence the SCADA system against the insider attack.

C. Network Configuration Management (NMC)

The world is now more of entrepreneur network ever since last five years. It provides various services such as web services, data or voice convergence and so on and so forth [10]. However, this network would often face downtime due to the failure of the system and/or lack of understanding of the system. The enterprises downtime always takes a long period of time to recover and hence leads to higher cost loss and low company reputation. In order to overcome the system downtime problems, configuration management is being introduced. It provides a centralized view of all the network elements in a multivendor network besides providing a uniform network element configuration. It also ensures faster and more accurate device configurations, changes and deployments. It is able to track network changes and instill accountability as well as able to quickly restore to a known and trusted state if any suspicious condition being spotted. To conclude, configuration management helps to increase security and business efficiency [10].

There are several types of network configuration management (NCM) introduced by different companies. To summarize, among the four NCMs compared, SolarWinds NCM, ManageEngine, rconfig and RANCID, only RANCID and rconfig are open source but RANCID is compatible to

Linux whereas rconfig is compatible to Windows. Due to the limited features and support given for free rconfig installation, RANCID was chosen to be the NCM and RANCID is easy to install and configure in Ubuntu, making it the suitable NCM used to manage devices in our scheme. Subversion and web-subversion features under RANCID are being used as well to organize information provided by each device and upload them to web browser.

IV. Methodology

A. Existing Methods

There are various solutions suggested or provided by different organizations on the Internet due to the urge of providing SCADA system a more complete security in order to make it more reliable and safer for the users as well as the businesses.

Firstly, LightCyber Company has introduced a LightCyber Magna to protect SCADA and industrial control system networks. It offers the system to detect suspicious code, login attempt, communication, as well as generating alerts of unsuccessful authentication attempt [11].

Secondly, IBM Security Identity Governance and Intelligence has provided a set of security protections which could provide an identity governance platform for owners to access and ensure regulatory compliance. It also provides a business-activity-based approach so as to avoid the duties violations across enterprise applications. Moreover, it gives the visibility and user access control by strengthening access entitlements from target applications and employing sophisticated algorithms [12].

Last but not least, CISCO has listed some advice to the users on the CISCO blog to raise awareness on methods to ensure a safe system used. Most of the rooms that stored the hardware systems were not being well protected against insider attack. The businesses were to be reminded to restrict the access to these crucial rooms as research has found that employees are less likely to conduct an attack in an environment that they knew they were being watched [13]. CISCO also reminded businesses to be careful in vetting each of the security guard's personal particulars, as well as to increase the number of guards and the amount of rotations. This is to reduce the risk of malicious attackes carried out by the attacker who took the chance by taking the job as a guard in the organization. Most importantly, businesses should conduct safety test internally every now and then to test the safety and reliability of its system. By carrying out penetration test and mock attack to the system, the organizations could identify their own weaknesses in defending the system against insider and outsider attacks [13], and thus improve their systems.

B. Proposed Ideas

It is crucial to protect the system from both internal and external attacks. The consequences of any malicious attacks could not only lead to the loss in monetary, confidential information, and human life, but also cause disaster in the organization, the arena, the country or even worldwide. Therefore, the solutions discussed and suggested in this section focus specifically on the scheme to protect the SCADA system against malicious insider attack.

1) If any suspicious act found, lock the particular user ID immediately. The system operator should be alerted while the system locks the suspicious user ID automatically. The operator should then proceed to check for the system security to make sure the suspicious act is not done by a malicious attacker.

2) For vendors or contractors, set a onetime account/password for them when necessary. This is to avoid the vendors or contractors to have the access to the system freely without the organization knowing or realizing. This could be applying in the organization to avoid a significant amount of attack from the vendors or contractors side.

3) Any critical area of the system should only be able to access by onetime password. This applies the same idea as the previous solution. The crucial area of the system no matter hardware or software, should be limit to only accessible by onetime password. Any request for the onetime password should be recorded and made traceable in case of any incident happens.

4) Backup system every day. By backing up system on daily basis, it gives the operators the opportunity of revising and realizing any changes made or updated along the day to the system. This could help the operators to spot any suspicious or unauthorized changes made to the system.

5) Traceable real-time script. Whenever someone is editing the system script, it will appear on the other side of the system on real-time basis where there are authorized operators to be monitoring. There are ways to run and execute a system program without the person appeared in front of the computer. An experienced programmer is able to set the execution at later timing even when he is not around. SCADA system should mute this function and make all the changes more transparent to everyone, eg the changes will be made and updated in real-time basis. Everyone in the group will be notified even before the changes are being updated, for example, when someone tries to access and make changes in the system, the group in charged should already be notified on this access. A notify message should be sent to the group in charged and they will be alerted and proceed to any necessary action.

6) Conduct safety test on certain routine. Test should be carrying out regularly. This is the more straight forward way on checking and ensuring safety of the system. Operators get to compare the configuration reports to see if any changes have been made and spot the suspicious part quickly.

C. Final solution

Fig. 5 shows a block diagram of the relationship of each suggestion with SCADA system. The first three ideas proposed are focusing on the password input to the system whereas the other two ideas are focusing more on the output from the system which consists of devices status.

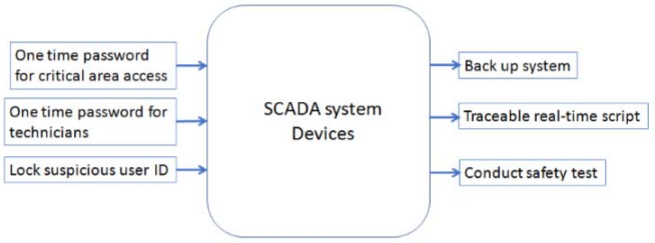

Figure 5. Block diagram of relationship of each suggestion with SCADA system

The feedback gathered from the SCADA system operators of the transportation company showed that they are less likely to notice their devices status, such as the devices connected to host, the IP address of the devices connected, as well as the condition of the devices, if they did not take the initiative in checking the status of their system. The inconvenience in noticing system changes makes the system vulnerable to malicious attacks.

Among the advices provided in CISCO blog, the most useful method to ensure the security of the equipment is to carry out safety test for the system regularly. As the testing could show if the system equipment are acting normally or work as expected. It is a simple yet useful method to detect any possible attack.

When most of the existing solutions are focusing on the controlling and protecting the system safety from the input to the system, this project decided to focus on protecting the output from the system instead. With the consideration on the effectiveness and efficiency of aforementioned suggestions, the proposed final solution would be, combining point 4, 5 and 6 from the proposed ideas, to make the changes traceable in real-time and to conduct safety test to the system on a regular basis besides backing up system every day. This solution focuses on the protection over the field equipment used in the SCADA system, which will be represented by routers, switches and host in the testing. By conducting such testing, it aims to make sure that the operators get notified and alerted if any of these devices is hacked or attacked. In order for the aim to be achieved, it requires the devices to reply a particular response that was set beforehand. The devices are expected to reply accordingly when the operator requested a response from each of them.

Fig. 6 shows the block diagram of the software and components involved in final system. GNS3 is used to build network topology which includes Cloud, Router, Switch and Host. Ubuntu is installed in VMware Workstation 12 player to code RANCID, SVN and webSVN. Network topology is linked to Ubuntu through VMware Network Adapter VMNet1. Further details are to be discuss in the below sub sessions.

V. Implementation

A. Network topology

The topology required is being built in GNS3 as shown in Fig. 7. It is a platform that allows users to simulate network protocol for designing and configuring according to real life simulation. It also allows emulation of CISCO IOS in a user-friendly interface. GNS3 is often being used to combine virtual and real devices for testing and troubleshooting complex simulation network.

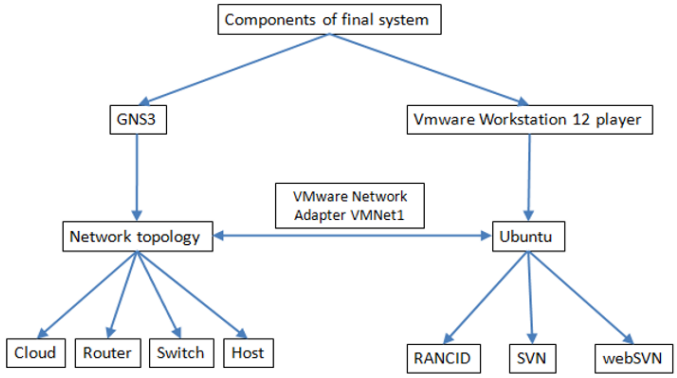

Figure 6. Components of final system

Network topology used in this project includes a cloud, a router, a switch and a host in the GNS3 platform. The topology is simulating the real CISCO devices being used in transportation control and configuration system. As shown in Fig. 7, Cloud is representing Ubuntu in this platform which is to be connected to one of the Ethernet port of Router. Its role is to link the RANCID in Ubuntu with the devices to be managed in GNS3 by transferring data from devices back to Ubuntu. Another Ethernet port of Router is connected to Switch. Router has only two ports whereas Switch has ten ports. Hence, Switch is usually being used in network topology to connect more than two devices. Other than the port connected to Router, only one port from Switch is being used in this topology, which is to connect to Host. The network topology is set up as shown in Fig. 7.

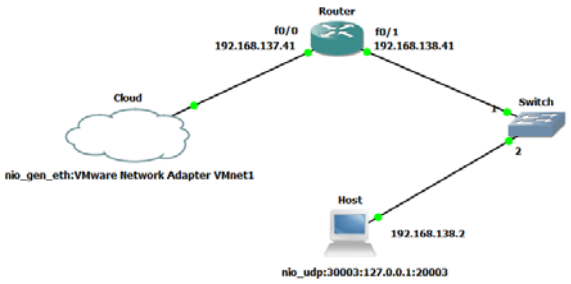

Figure 7. Network topology set up in GNS3

B. Ubuntu

Ubuntu is free software that is often used to operate in a virtual machine, in this case, the VMware Workstation 12 Player. Ubuntu also provides a free platform for documentary and discussion among its users to communicate and study from one another.

Other than RANCID, the SVN, an open source version control system that would help in managing files and folders is also being installed onto Ubuntu [14]. It helps to update

modifications to the web page and manages the configuration files and history in the browser. Besides, by installing webSVN, the browser can be set up with a nicer interface. It could be accessed by the authorized staff and operators and they will all be alerted if there are any suspicious changes being modified in the system. With the help of SVN and webSVN, the configured information of each device is able to be kept and managed in browser, which makes it convenient for the operator to keep track at any time.

In order to have Ubuntu in Windows PC, a VMware Workstation 12 Player is installed. It is an open source system which allows users to run multiple operating systems in single PC [15].

VI. Simulation Results

A. GNS3

It is crucial to ensure a stable and accurate connectivity between devices in the system. In the real-world transportation system which uses SCADA, their main control system may be made up of a few routers with switches connected to more than one host, through physical wired or internet linking. Hence, IP address plays a crucial role in allowing the devices to communicate among one another. Among devices used in this project network topology, Switch does not has its IP address as it just simply lets the data packages pass through it, from Router to Host or vice versa. Therefore, the connectivity test will be focus on Router and Host.

To test the connectivity between devices, simply "ping" IP address of the device you wish to communicate with. Once the "ping" result is 100% rates, it means that the devices are now all successfully connected and ready to communicate with one another.

B. Subversion and websubversion

By setting up RANCID together with subversion (SVN) and websubversion (webSVN), files which contain devices information will automatically be uploaded to the browser. Files uploaded to the browser can be viewed by the operator with authorized access. Any modification uploaded will update the "Last modified" date, time and author information in the browser, as shown in Fig. 8. The details information provided in each file uploaded to the browser includes device type, device IP address and number of devices connected. If there are any changes detected in any two revisions uploaded, a side by side comparison page as shown in Fig. 9 will be provided hence help the operator to identify the genuine of the modification.

VII. Conclusion

The method proposed and implemented in this project has placed its focus on the transportation system which uses SCADA for controlling and monitoring purposes. This project has demonstrated innovative strategies in the development of effective protection scheme against insider attack.

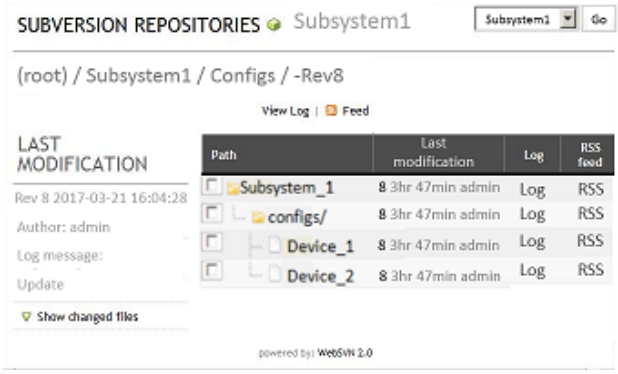

Figure 8. Subversion repository shows in browser

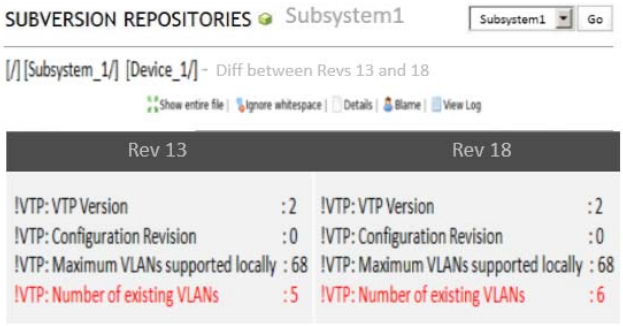

Figure 9. Side by side comparison page shows in browser

The implemented idea provides configuration report of the devices in SCADA system that could be accessed by the operators. Besides, it can ensure safety of each of the devices by checking data uploaded from them. If any of the data provided from devices is not as expected, the operator will be able to proceed to check for the nature of the modification made.

In providing traceable real-time script and conduct of safety test would allow the operators stay informed at all time. This method is believed to be useful in helping the organization to minimize the probability of insider conduct attack on the system. With the immediate alert, the organization would have sufficient time to react accordingly. By applying this scheme, the reliability of the system would be increased and the safety of the system would be guaranteed from insider attack since any changes made can be tracked and traced on real-time basis. As any suspicious modification made to the system will be notified to the operators, a quick response can be conducted to prevent any further damage dealt to the system. Moreover, backing up data everyday helps to ensure the database is always up-to-date and can always be referenced to when inspecting any suspicious changes found in the system.

Since it is not a tedious methodology in setting up the protection scheme towards the prevention of insider attack, there is a pressing need for the organization with such transportation system to implement the aforementioned protection scheme.

ACKNOWLEDGMENT

I would like to take this opportunity to express my sincere gratitude to my supervisor, A/Prof Wang Ling Guo for her continuous support and encouragement. I am extremely thankful to her for sharing expertise, patience, and invaluable guidance extended to me.

My sincere thanks also goes to my RI co supervisor, Dr Huaqun Guo, at Institute of Infocomm Research (I^2R), Agency of Science, Technology and Research, (A*STAR) for her immense knowledge and insightful comment on the research field. Thanks also goes to Mr Zhigang Zhao, the I^2R engineer for his willingness to help when I faced issues during this project especially regarding the software issues.

Last but not least, I am grateful to have wonderful family and friends, who directly or indirectly, lent their hand in this venture.

REFERENCES

[1] V. Prabhu, "Anonymous hack Pentagon, NY Times, US Military and leak email ids and phone numbers » TechWorm", TechWorm, 2017. [Online]. Available: https://www.techworm.net/2014/03/anonymous-hack-pentagon-ny-times-us.html. [Accessed: 06- Apr- 2017].K. Iyer, "8 Most Amazing and Daring Hack Attacks Carried Out By Anonymous", TechWorm, 2016. [Online]. Available: https://www.techworm.net/2016/01/8-amazing-daring-hack-attacks-carriedanonymous.html. [Accessed: 06- Mar- 2017].

[2] J. Harp, "Anonymous declares war on Trump", Digital Spy, 2015. [Online]. Available: http://www.digitalspy.com/tech/news/a777013/anonymous-declares-war-on-donaldtrump-think-twice-before-you-speak/. [Accessed: 16- Mar- 2017].

[3] W. Shaw, Cybersecurity for SCADA system, 1st ed. 2006, p. Chapter 7.

[4] T. Agarwal, "SCADA System Architecture, Types and Applications", Edgefx Kits Official Blog, 2017. [Online]. Available: http://www.edgefxkits.com/blog/scada-systemarchitecture-types-applications/. [Accessed: 10 Mar 2017].

[5] "What is SCADA? Supervisory Control and Data Acquisition", Inductiveautomation.com,2017.[Online].Available:https://inductiveautomation.com/wha t-is-scada. [Accessed: 10 Mar 2017].

[6] "SCADA System", Electronics Hub, 2015. [Online]. Available: http://www.electronicshub.org/scada-system/. [Accessed: 10- Mar- 2017].

[7] "What is a Remote Terminal Unit (RTU)? - Definition from Techopedia", Techopedia.com,2017.[Online].Available:https://www.techopedia.com/definition/1033/r emote-terminal-unit-rtu. [Accessed: 10 Mar 2017].

[8] "SCADA Human Machine Interface (HMI) for Viewing and Controlling Remote Telemetry Units", Dpstele.com, 2017. [Online]. Available: http://www.dpstele.com/ scada/hmi.php. [Accessed: 10 Mar 2017].

[9] 2015. [Online]. Available: http://www.securonix.com/insider-attacks-were-the-mostcostly-breaches-of-2015/. [Accessed: 12 Mar 2017].

[10] Z.Kerravala, As the value of Enterprise Network escalates, so does the need for Configuration Management, January 2004.

[11] 2017.[Online].Available:http://lightcyber.com/wpcontent/uploads/2017/01/Light Cyber_Protecting_SCADA_SB.pdf. [Accessed: 12 Mar 2017].

[12] "IBM Security Identity Governance and Intelligence", Www-03.ibm.com, 2017. [Online]. Available: http://www-03.ibm.com/software/products/en/ibm-securityidentity-governance-and-intelligence. [Accessed: 1 Mar 2017].

[13] N. Leali, "Lessons From an Insider Attack on SCADA Systems", blogs@Cisco– CiscoBlogs, 2009. [Online]. Available: http://blogs.cisco.com/security/lessons_from_an_insider_attack_on_scada_systems. [Accessed: 12 Mar 2017].

[14] R. K., "How to Install Subversion Server on Ubuntu 16.04 & 14.04 LTS", TecAd-min.net, 2016. [Online]. Available: https://tecadmin.net/install-subversionserver-on-ubuntu/#. [Accessed: 14 Mar 2017].

[15] “Workstation for Windows”, VMware product, 2017. [Online] Available:http://www.vmware.com/products/workstation.html.Accessed: 1 Mar 2017].