A secured tor local network for nuclear power plant industry

Vinodh Kumar C, Rajasekar B, Balasankar Karavadi and Premalatha J

1, 4School of EEE, Sathyabama Institute of Science and Technology, Chennai, India
2School of EEE, Sathyabama Institute of Science and Technology, Chennai, India
3Dept of Biomedical Engg, Sathyabama Institute of Science and Technology, Chennai, India

E-mail:vino83pc@gmail.com

Abstract. The risk of cyber-attacks on a country has grown drastically. The cyber security risks against critical power infrastructure seem to be worsening. Obviously, any sort of assault on an atomic plant is very concerning. An attack that allows hackers to manipulate the system that control a nuclear reactor, while very difficult, could have very serious consequences. The main reason for this attack is vulnerabilities in local computer networks in power plants. Which has direct access to the internet without any major protection against cyber-attacks like phishing attacks against power plant employees, virus injection tools etc., As the main defense against this attacks is to make power plant networks and employees anonymous to the internet and making sure that no one is tracking the employees which can lead to loss of sensitive information of the plant. The Tor onion networking protocol is best suitable for these types of attacks on employees and computer networks in the power plant. Since providing Tor network for individual employee in practically impossible. Our projected work aims to establish an onion router which provide overall coverage of computer systems and employees which has access to power plant inside the perimeter of power plant. To simulate the plant local networks we construct an internet router using raspberry pi which is configured with Tor onion routing protocol access the internet by computers connected to our Router.

1. Introduction

The existing local network system does not include any standard encryption methods to secure the power plant local network which makes them venerable to cyber-attacks. An assault that permits programmers to control the frameworks that control an atomic reactor, while troublesome, could have intense outcomes. The main reason for this attack is vulnerabilities in local computer networks in power plants. Disadvantages of existing system are 1) Need install of security systems separately for every local network.2) Vulnerable to cyber-attacks. 3) Hackers can intercept power plant networks and 4) Outdated security measures.

Using the TOR router built using the raspberry pi encrypts your traffic and protects your privacy no matter what network you are using. If Ethernet is not available, your router can connect to a Wi-Fi network in addition to creating its own, acting as a bridge between your personal Wi-Fi access point and unsecured Wi-Fi33. Here we proposes such a system to protect the network of a power plant Advantages of Proposed Tor Network are 1) Make networks hack proof 2) Flexibility to update with modern security technology 3) Impossible to trace and 4)Military grade protection.
2. System Modules and Configuration of Proposed Local Network

A secluded Modules diminishes intricacy, facilities change (a basic part of programming viability), and results in simpler usage by empowering equal improvement of various piece of framework. Programming with successful particularity is simpler to create in light of the fact that capacity might be compartmentalized and interfaces are improved. Programming engineering encapsulates seclusion that is programming is isolated into independently named and addressable segments considered modules that are incorporated to fulfill issue necessities. Seclusion is the single quality of programming that permits a program to be mentally sensible. The five significant rules that empower us to assess a plan strategy concerning its capacity to characterize a viable measured plan are Modular decomposability, Modular Comps ability, Modular Understand ability, Modular continuity, Modular Protection.

The following are the modules of the projected work, which is planned in aid to complete the project with respect to the proposed system, while overcoming existing system and also providing the support for the future enhancement. Programming with viable particularity is simpler to create on the grounds that capacity might be compartmentalized and interfaces are improved. Programming design typifies measured quality that is programming is isolated into independently named and addressable parts called modules. Rundown of Modules are given beneath.

- Configuration of access point.
- Install the Tor.
- Configure Tor.
- Delete the old IP Tables and replace with new ones.
- Route DNS through the TOR.
- Check the status of tor service.
- Reboot.

2.1. Configuration of Access Point

The product design for a passageway is somewhat more included, yet not extremely muddled. It's normally done by means of a Web interface. To get to the arrangement page for the passage, you have to realize the passageway's IP address. At that point, you simply type that address into the location bar of a program from any PC on the organization. Multifunction passageways typically give DHCP and NAT administrations to the organizations and twofold as the organization's door switch. Therefore, they commonly have a private IP address that is toward the start of one of the Internet's private IP address ranges, for example, 192.168.0.1 or 10.0.0.1. Counsel the documentation that accompanied the passageway to discover more. At the point when you access the arrangement page of your remote passageway on the Internet, you have the accompanying setup choices that are identified with the remote passageway elements of the gadget. Despite the fact that these alternatives are explicit to this specific gadget, most passageways have comparative setup choices.

2.2. Architecture of Tor Network

The overall architecture of Tor network is shown in figure 1. First the computer to be connected to the internet modem and modem is connected to the internet service provider (ISP). The whole process is done with the Tor network with several Tor exit nodes and the data packets are transferred from one node to the other using onion routing protocol which makes it impossible to trace back the signal form one node to the other.
2.3. Encryption Process of Tor Network

Onion Routing is a method for unknown communication over a PC organization. In an onion network, messages are encapsulated in layers of encryption, analogous to layers of an onion which is shown in figure 2. The encoded information is communicated through a progression of organization hubs called onion switches, every one of which "strips" away a solitary layer, revealing the information's next objective. At the point when the last layer is unscrambled, the message shows up at its objective. The sender stays mysterious in light of the fact that every delegate knows just the area of the quickly going before and following hubs. The onion routing provides a high level of security.

There is a large set of precautionary measures and best practices to make web browsing safer and more secure for users. That you send a HTTPs request to a server and someone intercepts that request but that person can’t know what that message says because it’s encrypted. But you are still not with this level of security and want to take this to the next level i.e. don’t even want anyone sing on your network to know which server you are contacting and if you are making any requests or not. This is where onion routing comes in.

3. Installation of Tor Router and Configuration of Raspberry Pi

The completion of the Raspberry pi Tor router provides the WI-FI signal as internet hotspot which protects the data traffic through implementation of Tor network service. The Tor Router is a mix of raspberry pi 3 based hardware and modified raspbian operation system software.
The installation of tor router (fig.3) consists of several modules. The following are the modules of the projected work, which is planned in aid to complete the system with respect to the proposed system, while overcoming existing system and also providing the support for the future enhancement. Programming with powerful seclusion is simpler to create on the grounds that capacity might be compartmentalized and interfaces are rearranged. Programming design exemplifies seclusion that is programming is partitioned into independently named and addressable segments called modules. To connect to raspberry pi one has to use one of the ways to interconnect raspberry pi to local network of computer.

SSH (Secure Shell) is one of the ways to connect to raspberry pi for future configurations to apply. IP address of the pi should be known for the SSH connection establishment. Raspbian is the operating system for raspberry pi which is shown in figure 4.
3.1. Installation and Configuration of Tor network

To get to the design page for the passage, you have to realize the passageway's IP address. The installation (fig.6) of Tor network in the raspberry pi through connection SSH (Secure Shell).

The Tor network should be configured with the raspbian operating system for the normal flow of data traffic without error. The oldest IP Tables must be replaced with the new ones which are implemented by Tor network as shown in figure 7.
After the completion of configuration the Tor service must be rebooted and the Tor status (fig.8) must be noted for proper configuration.

Figure 8. Tor status.

The Tor service is enabled as shown in figure 8, if the configuration of Tor is not properly installed then the Tor service status should have shown as error in configuration. The designers of the Tor network have placed a great deal of emphasis on achieving low latency and reasonable throughput in order to allow interactive applications, such as web browsing, to take place within the network. To make and communicate an onion, the originator chooses a lot of hubs from a rundown gave by an “index hub”. The picked hubs are orchestrated into a way, called a “chain” or "circuit", through which the message will be sent. To preserve the anonymity of the sender, no node in the circuit is able to tell whether the node before it is the originator or another intermediary like itself. Similarly, no hub in the circuit can tell the number of different hubs is in the circuit and just the last hub, the "leave hub", can decide its own area in the chain.

4. Results from Web Monitoring Tool and Performance Analysis

Web monitoring is the way toward testing and confirming that end-clients can cooperate with a site or web application true to form. Site observing is regularly utilized by organizations to guarantee site uptime, execution, and usefulness is true to form. Site checking organizations give associations the capacity to reliably screen a site, or worker work, and see how it reacts. The checking is regularly led from a few areas around the globe to a particular site, or worker, so as to distinguish issues identified with general Internet idleness, network bounce issues, and to forestall bogus positives brought about by neighborhood or between interface issues. Checking organizations by and large report on these tests in an assortment of reports, diagrams and charts. At the point when a mistake is recognized checking administrations convey alarms by means of email, SMS, telephone, SNMP trap, pager that may incorporate analytic data, for example, an organization follow course, code catch of a site page's HTML record, a screen shot of a page, and even a video of a site coming up short. These diagnostics permit network directors and website admits to address gives quicker. Observing accumulates broad information on site execution, for example, load times, worker reaction times, page component execution that is frequently dissected and used to additionally upgrade site execution.

4.1. Data Monitoring before Tor

The Figure 9 shows the data traffic been captured by the Wireshark web monitoring tool before the Tor service been enabled in the raspberry pi WI-FI router.  The data show by the Wireshark web monitoring tool is the real time data been transferred by the router which contains the ip address, to ip address, from ip address, location details number of packets been transferred, ping time and all the search requests from any browsers of internet. This data indicates our privacy in the digital world which can simply compromised by and hacker how known where to look.
4.2. Data Monitoring after Tor
The Figure 10 shows the data traffic been captured but has been encrypted by Tor. The Wireshark web monitoring tool after the Tor service has been enabled in the raspberry pi WI-FI router. The data show by the Wireshark web monitoring tool is the real time data been transferred by the router which contains the IP address, to IP address, from IP address, location details number of packets been transferred, ping time and all the search requests from any browsers of internet are been encrypted using onion routing protocol by Tor network which makes the data captured is of no use.

This makes us anonymous in the internet and works the following functions: a) it provides secure browsing environment. While browsing the internet it is often not secure and allows your browsing history or path to fall in to the wrong hands thereby violating your privacy. b) Secure email accessing. Emails can be hacked by hackers or spies hence it is essential to keep the email access encrypted by this TOR router. c) To make power plant networks anonymous for the internet and to prevent any cyber-attacks.
5. Conclusion

Thus, the projected work infer that all the computer networks in country’s critical infrastructure are
protected from hackers and hacking organizations and cyber-attacks which if left to ignore leads to
critical infrastructure failure and may cripple the country’s defense. The protection is given by
integration of Tor networks which uses onion routing protocol and shifting of all the internet traffic
through these Tor networks. The Tor networks make sure of the encryption which make the power
plant networks anonymous in the public internet and make the networks untraceable and hack proof
in terms of protection and privacy which can significantly drop the risk of cyber-attack on our nuclear power
plants.

6. References

[1] Bauer, K, McCoy. D, Grunwald. D, Kohno. T, Sicker. D, “Low-resource routing attacks against Tor”, Proceedings of
the Workshop on Privacy in the Electronic Society, Washington, DC, USA, Vol.6, No.2, October 2007, pp.11-20.
[2] Bethencourt. J, Franklin. J, Vernon. M, “Mapping Internet sensors with probe response attacks”, Proceedings of the 14th
conference on USENIX Security Symposium, Baltimore, MD, USENIX Association, Vol.24, No.5, July 2005,
pp.193-208.
[3] Cesari. P, “Caught in the Network”, The Chronicle of Higher Education, Washington, D.C, Vol.53, No.3, February
2007, pp.92-98.
[4] Dingledine. R, Mathewson. N, Syverson. P, “Tor: The second-generation onion router”, Proceedings of the 13th
USENIX Security Symposium, Vol.8, No.1, August 2004, pp.1-17.
[5] Feamster. N, Dingledine. R, “Location diversity in anonymity networks”, Proceedings of the 13th USENIX Security Symposium, Vol.8, No.1, August 2004, pp.1-9.
[6] Goldberg. I, “On the security of the Tor authentication protocol”, Proceedings of the Sixth Workshop on Privacy
Enhancing Technologies, Cambridge, UK, Springer, Vol.6, No.7, June 2006, pp.28-34.
[7] Goldschlag. D.M, Reed. M.G, Syverson. P.F, “Hiding routing information”, Proceedings of Information Hiding: First
International Workshop, Springer-Verlag, LNCS 1174, Vol.32, No.8, May 1996, pp.1-24.
[8] McCoy. D, Bauer. K, Grunwald. D, Tabriz. P, Sicker. D, “Shining light in dark places”, A study of anonymous network
usage, University of Colorado Technical Report CU-CS-1032-07, pp.6-14.
[9] Murdoch. S.J, Danezis. G, “Low-cost traffic analysis of Tor”, Proceedings of the 2005 IEEE Symposium on Security and
Privacy, Vol.3, No.1, May 2005, pp.34-59.
[10] Murdoch. S.J, “Hot or not: Revealing hidden services by their clock skew”, 13th ACM Conference on Computer and
Communications Security, Alexandria, VA, November 2006, pp.1-16.
[11] Overlier. L, Syverson. P, “Locating hidden servers”, Proceedings of the 2006 IEEE Symposium on Security and Privacy,
IEEE CS, Vol.7, No.2, May 2006, pp.9-18.
[12] Shinoda. Y, Ikai. K, Itoh. M, “Vulnerabilities of passive Internet threat monitors”, Proceedings of the 14th Conference on USENIX Security Symposium, Baltimore, MD, USENIX Association July 2005, pp.1-14.
[13] Sicker. D.C, Oh. P, Grunwald. D, “Legal issues surrounding monitoring during network research”, Proceedings of the
7th ACM SIGCOMM conference on Internet measurement, New York, NY, USA, Vol.2, No.5, Oct 2007, pp.4-12.
[14] Vinothkumar.C, “An automated surveillance and procontrol system for vacuum pump instrumentation in power plant
industries”, International Journal of Applied Engineering Research, Vol.9, No.24, (2014), pp.30759-30770.
[15] Wendolsky. R, Herrmann. D, Federrath. H, “Performance comparison of low-latency anonymity services from a
user perspective”, Proceedings of the Seventh Workshop on Privacy Enhancing Technologies, Ottawa, Canada,
Springer, Vol.6, No.3, June 2007, pp.4-15.