Attack Tree Design and Analysis of Offshore Oil and Gas Process Complex SCADA System

M. V. V. Siva Prasad
Research Scholar, Department of Computer Science & Systems Engineering,
AU College of Engineering (A), Andhra University, Visakhapatnam

P. S. Avadhani
Professor, Department of Computer Science & Systems Engineering,
AU College of Engineering (A), Andhra University, Visakhapatnam

ABSTRACT

Attack Trees are very important in the effort to secure Industrial Process Control Systems (ICS), because they aid directly in indicating the presence of vulnerabilities in network and how attackers use the vulnerabilities to implement an effective attack. Attack Tree design and analysis provide clues for the network security professionals on how an attacker exploits the vulnerability on the network to achieve goals. In this paper it will be illustrated for designing attack tree in Offshore Oil and Gas Process Complex SCADA System to identify various vulnerabilities. Using the vulnerabilities it presents how an attacker can take control of the SCADA system network and eventually affect hydrocarbons production.

Keywords

ICS, SCADA, MTU, TDMA, RTU

1. INTRODUCTION

SCADA system network instrumentation and control are critical for offshore oil and gas process complex as they support the operational state of the process complex via interaction with remote platform physical transducers and equipment. They are also responsible for oil and gas process control at remote platforms. SCADA systems are operated in environments different from those of conventional IT systems. In the past, SCADA systems were based on analog technologies; however, since the introduction of digital technologies in the 2000s, the proportion of digital technologies has been steadily increasing. The Present study SCADA system implemented in Tier structure is on corporate LAN. Since corporate LAN is not isolated the SCADA system exposed to network attacks. To access the impact of various threats faced by networks utilizing vulnerabilities Attack Tree analysis is proposed and developed by Schneier [1]. Phillips and Swiler in 1998 outlined a method that used graph to evaluate network security risk [2]. Meadows in his paper proposed using a graph representation to model stages of attacks on cryptographic protocols [3]. There is one approach of building security scenario on graph theory based graph assessment. According to Ramakrishman etal [4] graph theory based model checking was initially used to analyze whether a given goal state is reachable from the initial state and model based attack graph assessment used to enumerate all possible sequences of attacks between the two states. Ammann etal [5] in their paper proposed more compact representation of attack graph was proposed based on the graph theory in 2005. The attack tree analysis developed to assess the vulnerability of systems to a specific attack and security test. In general, the root nodes of attack trees and attack graphs represent the goal of an attack, other nodes represent the vulnerability that is exploited by the attack, and edges represent the relationship between nodes. In calculating the achievement probability of attack goals and to identify detailed attack routes, Ammann etal in his paper presents the attack model can be extended says [5] by introducing success probability or occurrence probability. Attack Trees node analysis can be obtained according to Poolsappasit etal [6] and Ivanc etal [7] using AND/OR conditions in the nodes or edges. A commercial tool SecurI Tree [8] developed by Amaneza Tech Limited for risk analysis using attack tree modeling analysis. And one rudimentary tool developed by Alexander Opel, Design and implementation of a Support Tool for Attack Trees [9]. Similarly TANAT-Threat ANd Attack Tree Modeling plus simulation [10] is one rudimentary tool for attack tree modeling already available for Schneier's attack trees. Stefan Einarsson & Marvin Rausand in their paper presented the concept of vulnerability of complex industrial systems how it is defined and discussed in relation to risk and system survivability [11]. According Jan Stefan and Markus Schumacher in their paper compared common methods of sharing security related knowledge with regard to their ability to support avoidance and discovery of vulnerabilities. They proposed a collaborative attack model that is suitable for above purpose. This method combines a graph based attack modeling technique with ideas of web based collaboration tool [12]. In his paper J.P.Mcdermott, using Petri net for penetration testing model is quite useful. It retains the key advantages of flaw hypothesis and attack tree approaches [13]. Attack trees found to great aid in threat analysis. Attack trees not yet provided with an unambiguous semantics. Sjouke Mauw and Martin Oostadijk argue that such a formal interpretation is must to understand how attack trees can be manipulated during design and analysis proposed a denotational semantics, based on a mapping to attack suites [14]. The attack goal of the attack tree and attack graph is limited to a single root node defined in advance; therefore, it is difficult to predict the processes and results of various attacks, from various angles. In order to design attack trees and attack graphs, asset identification and analysis have to be performed first to acquire information regarding the operating environment and specific vulnerabilities of the target system or network. Attack Tree threat modeling involves understanding the complexity of the system and identifying all possible vulnerabilities and threats to the system, regardless of whether or not they can be exploited. Proper identification of vulnerabilities or threats and appropriate selection of countermeasures reduces the ability of attackers to access and control the system.

2. METHODOLOGY TO CONSTRUCT OFFSHORE OIL AND GAS PROCESS COMPLEX SCADA ATTACK TREE

Attack trees constitute a powerful security tool aimed at modeling the many ways in which an attacker may compromise different assets in a network. An attack tree provides a method for representing attacks (and similar vulnerabilities) on a system in the structure of a tree. The goal of the tree is the root node. The leaf nodes represent different paths to achieve the goal. In the proposed attack tree for SCADA system identifies the threats that might affect Offshore Oil and Gas Process Complex process control system network and potentially compromise its assets. This includes SCADA system Tier-1 network, host, and applications. Network vulnerabilities or threats can be assessed by investigating how the data passes through Tier-1network routers, firewalls, switches, and other network devices. SCADA system Engineer needs to understand the logic and syntax of these device's configuration files. In addition, system engineer needs to be able to determine what it takes to get past or compromise each device. Host investigations should include common configuration categories applicable to all server and operating system resources (patches, files/directories, ACLs).

To evaluate security of SCADA network, hosts security analyst must take into account the effects of local vulnerabilities and determine global security flaws. Scanning tools associated with Tier-1 SCADA system determine individual vulnerabilities of hosts. Using this information along with other information about network attack tree has been designed. The process for designing an attack tree for a SCADA system starts with important four servers Application Server, Web Server, Primary Server and Secondary Server's vulnerabilities. Each path in an attack tree is a series of exploits they may be called as actions. Actions lead to undesired state. An undesired state is a state where intruder has gained administrative control over the critical host. Each branch in the attack tree implies lone intruder action. A path from root node to any other leaf node down below action corresponds to action scenario. Modeling the attack tree involves associating a logical AND & a logical OR with each node. In essence, a node of an attack tree can be decomposed into an AND or an OR node. An AND node or an OR node decomposition can be represented in graphical or textual formats. Let us consider Tier-1 SCADA system implemented at process complex level and analyze the same with attack tree. Figure 1 is SCADA network diagram at Tier-1.

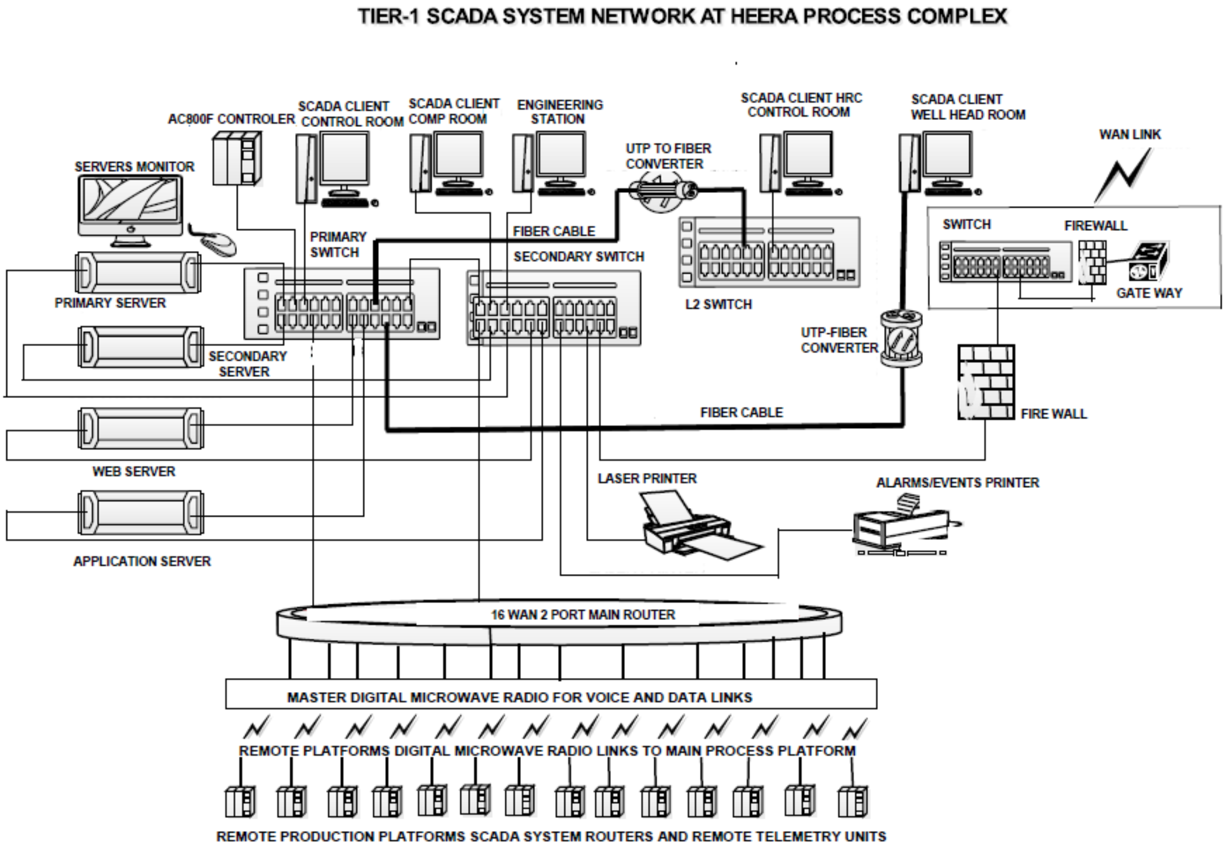

TIER-1 SCADA SYSTEM NETWORK AT HEERA PROCESS COMPLEX
AC800F CONTROLER
SCADA CLIENT CONTROL ROOM
SCADA CLIENT COMP ROOM
ENGINEERING STATION
SCADA CLIENT HRC CONTROL ROOM
SCADA CLIENT WELL HEAD ROOM
WAN LINK
SERVERS MONITOR
UTP TO FIBER CONVERTER
PRIMARY SWITCH
FIBER CABLE
SECONDARY SWITCH
SWITCH
FIREWALL
GATE WAY
PRIMARY SERVER
L2 SWITCH
SECONDARY SERVER
UTP-FIBER CONVERTER
FIBER CABLE
FIRE WALL
WEB SERVER
LASER PRINTER
ALARMS/EVENTS PRINTER
APPLICATION SERVER
16 WAN 2 PORT MAIN ROUTER
MASTER DIGITAL MICROWAVE RADIO FOR VOICE AND DATA LINKS
REMOTE PLATFORMS DIGITAL MICROWAVE RADIO LINKS TO MAIN PROCESS PLATFORM
REMOTE PRODUCTION PLATFORMS SCADA SYSTEM ROUTERS AND REMOTE TELEMETRY UNITS

Fig 1: Tier-1 SCADA System at Heera Offshore Oil and Gas Process Complex

The above figure 1 depicts SCADA system implemented at process complex level. It comprises of four Servers primary, secondary, WEB, and Application respectively. The Networking part includes with 16 WAN 2 Port main router and three numbers network switches. Main Telemetry Unit comprises of AC 800F main controller and Master Time Division Multiple Access (TDMA) Radio and Main Router. Master radio establishes communication links with remote platforms for field level data and parameters for necessary monitoring and control. Once Attack Tree is designed it's traversal along it' path gives access over different nodes. Which represent the vulnerabilities in attacker's way to gain control over the network.

A flow chart developed to generate for attack tree / graph given is below. The flow chart has basic principles as follow: First save the node which represents an attacker's host into an empty node queue. Second if the pointer of node queue not null, the host pointed to by the pointer will be considered as a host attacker to exploit this. From the host that is directly connected to the host of attacker, one can find the host which can be attacked by an attacker. If they are found, and they are not in node_queue, put each of them in the node_queue. That means an attack has occurred from the attacker's host to a new host. At the same time, the pointer will point to other elements in the next node_queue next to attacker's host. The third point is continuing step (2), until node_queue pointer is null, which means no more elements in the node_queue. At this point, the flow chart will end. A detailed explanation of the flow chart is shown in Figure below.

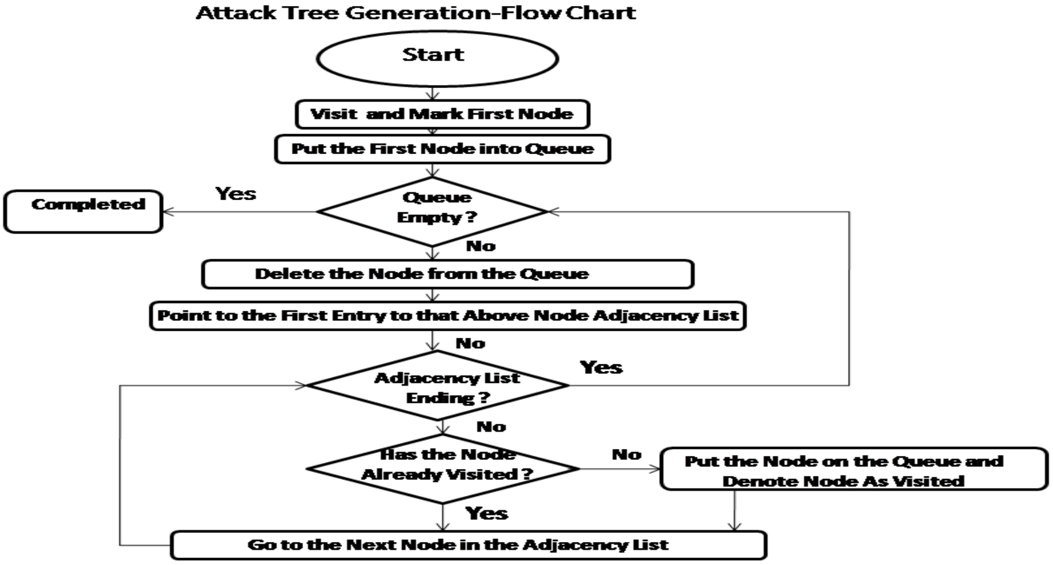

Attack Tree Generation-Flow Chart
Start
Visit and Mark First Node
Put the First Node into Queue
Queue Empty ?
Yes
Completed
No
Delete the Node from the Queue
Point to the First Entry to that Above Node Adjacency List
No
Adjacency List Ending ?
Yes
No
Has the Node Already Visited ?
No
Put the Node on the Queue and Denote Node As Visited
Yes
Go to the Next Node in the Adjacency List

Fig 2: Attack Tree Generation Flow Chart

3. ATTACK TREE DESIGN FOR GAIN ACCESS TO SCADA SYSTEM

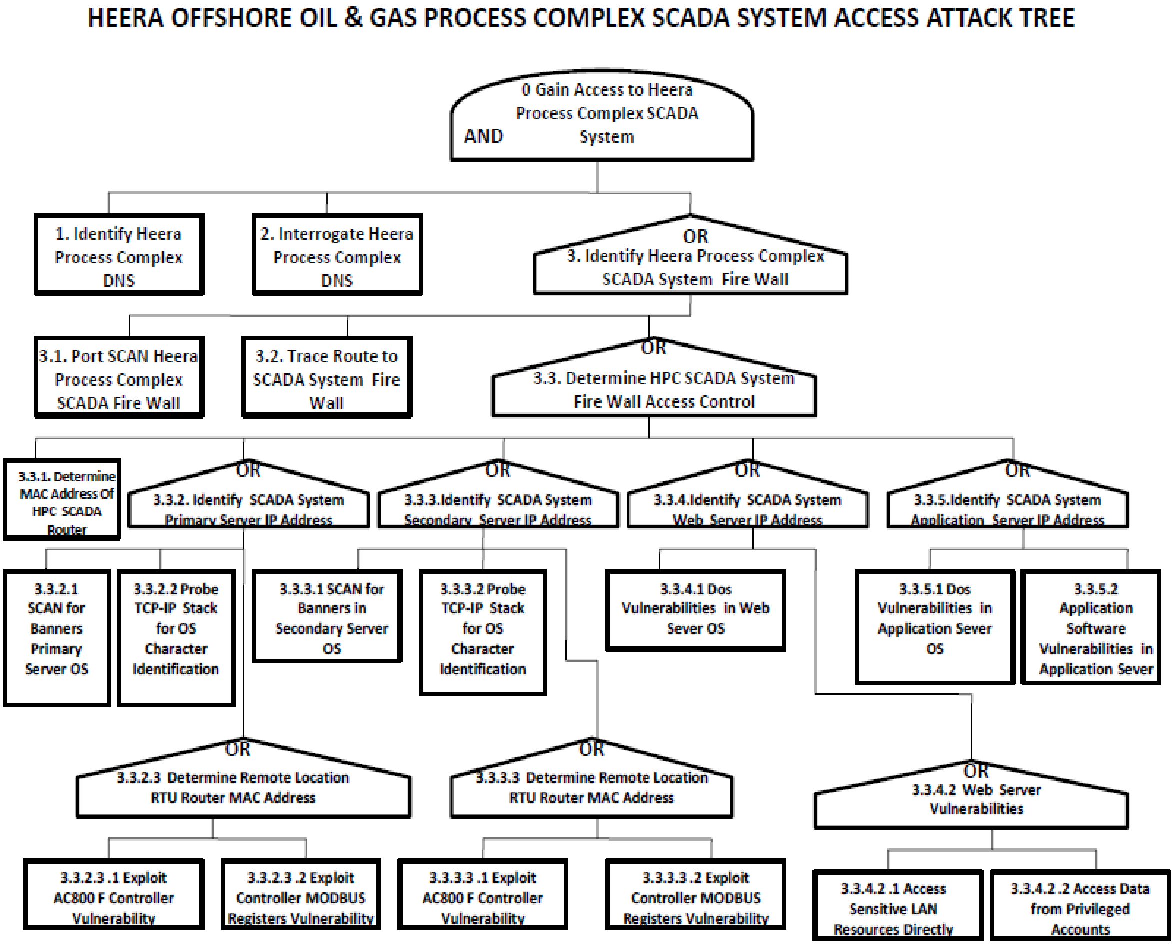
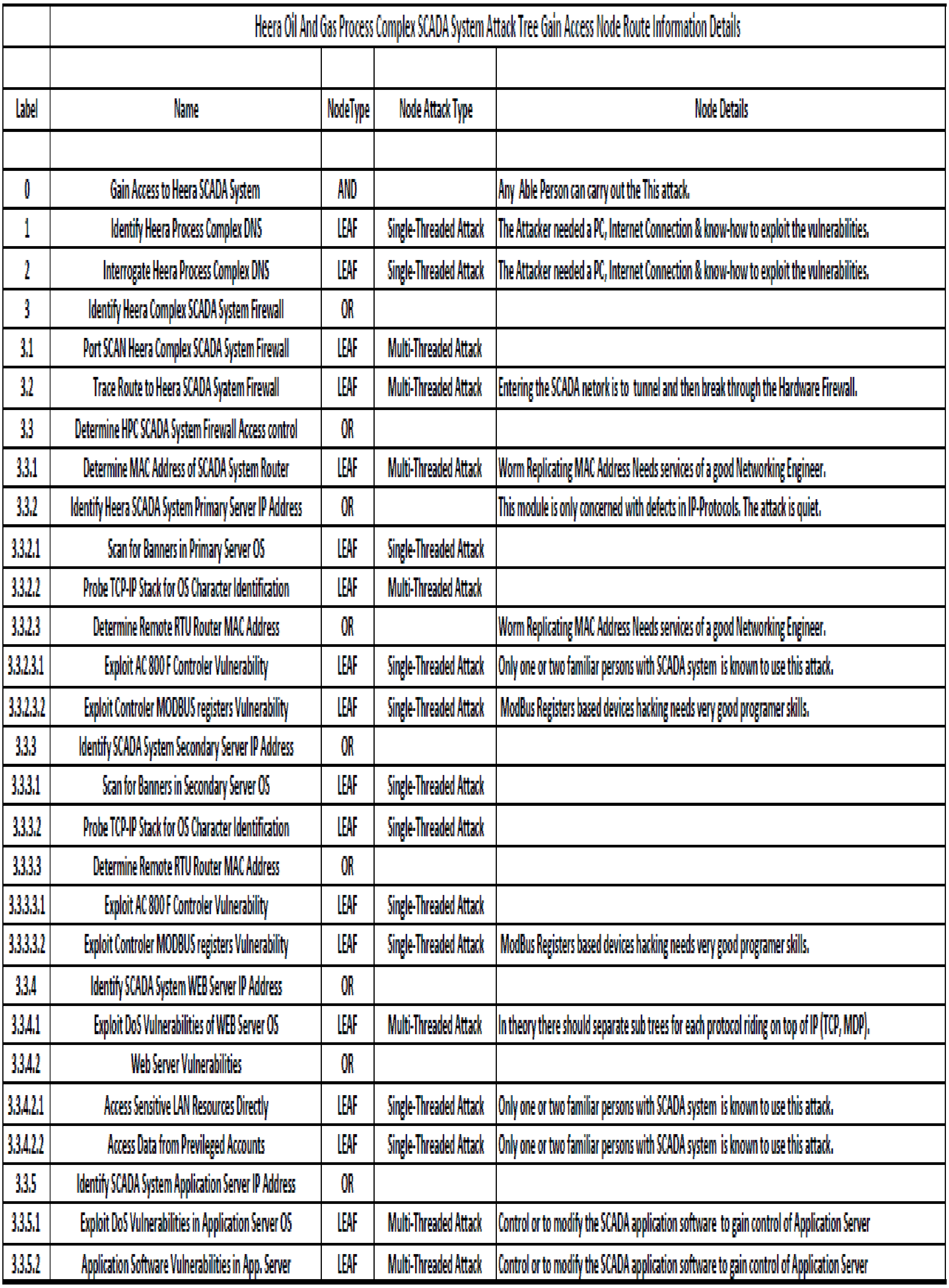

HEERA OFFSHORE OIL & GAS PROCESS COMPLEX SCADA SYSTEM ACCESS ATTACK TREE
0 Gain Access to Heera Process Complex SCADA System
AND
1. Identify Heera Process Complex DNS
2. Interrogate Heera Process Complex DNS
OR
3. Identify Heera Process Complex SCADA System Fire Wall
3.1. Port SCAN Heera Process Complex SCADA Fire Wall
3.2. Trace Route to SCADA System Fire Wall
OR
3.3. Determine HPC SCADA System Fire Wall Access Control
3.3.1. Determine MAC Address Of HPC SCADA Router
OR
3.3.2. Identify SCADA System Primary Server IP Address
OR
3.3.3.Identify SCADA System Secondary Server IP Address
OR
3.3.4.Identify SCADA System Web Server IP Address
OR
3.3.5.Identify SCADA System Application Server IP Address
3.3.2.1 SCAN for Banners Primary Server OS
3.3.2.2 Probe TCP-IP Stack for OS Character Identification
3.3.3.1 SCAN for Banners in Secondary Server OS
3.3.3.2 Probe TCP-IP Stack for OS Character Identification
3.3.4.1 Dos Vulnerabilities in Web Sever OS
3.3.5.1 Dos Vulnerabilities in Application Sever OS
3.3.5.2 Application Software Vulnerabilities in Application Sever
OR
3.3.2.3 Determine Remote Location RTU Router MAC Address
OR
3.3.3.3 Determine Remote Location RTU Router MAC Address
OR
3.3.4.2 Web Server Vulnerabilities
3.3.2.3 .1 Exploit AC800 F Controller Vulnerability
3.3.2.3 .2 Exploit Controller MODBUS Registers Vulnerability
3.3.3.3 .1 Exploit AC800 F Controller Vulnerability
3.3.3.3 .2 Exploit Controller MODBUS Registers Vulnerability
3.3.4.2 .1 Access Sensitive LAN Resources Directly
3.3.4.2 .2 Access Data from Privileged Accounts

Fig: 3 Offshore Oil and Gas Process Complex SCADA System Attack Tree

4. ATTACK TREE TOTAL NODES FOR GAIN ACCESS TO SCADA SYSTEM

Table: 1 Heera Oil and Gas Process Complex Attack tree Gain Access Nodes Detailed Information



	Heera Oil And Gas Process Complex SCADA System Attack Tree Gain Access Node Route Information Details			
Label	Name	NodeType	Node Attack Type	Node Details
0	Gain Access to Heera SCADA System	AND		Any Able Person can carry out the This attack.
1	Identify Heera Process Complex DNS	LEAF	Single-Threaded Attack	The Attacker needed a PC, Internet Connection & know-how to exploit the vulnerabilities.
2	Interrogate Heera Process Complex DNS	LEAF	Single-Threaded Attack	The Attacker needed a PC, Internet Connection & know-how to exploit the vulnerabilities.
3	Identify Heera Complex SCADA System Firewall	OR		
3.1	Port SCAN Heera Complex SCADA System Firewall	LEAF	Multi-Threaded Attack	
3.2	Trace Route to Heera SCADA Syatem Firewall	LEAF	Multi-Threaded Attack	Entering the SCADA netork is to tunnel and then break through the Hardware Firewall.
3.3	Determine HPC SCADA System Firewall Access control	OR		
3.3.1	Determine MAC Address of SCADA System Router	LEAF	Multi-Threaded Attack	Worm Replicating MAC Address Needs services of a good Networking Engineer.
3.3.2	Identify Heera SCADA System Primary Server IP Address	OR		This module is only concerned with defects in IP-Protocols. The attack is quiet.
3.3.2.1	Scan for Banners in Primary Server OS	LEAF	Single-Threaded Attack	
3.3.2.2	Probe TCP-IP Stack for OS Character Identification	LEAF	Multi-Threaded Attack	
3.3.2.3	Determine Remote RTU Router MAC Address	OR		Worm Replicating MAC Address Needs services of a good Networking Engineer.
3.3.2.3.1	Exploit AC 800 F Controler Vulnerability	LEAF	Single-Threaded Attack	Only one or two familiar persons with SCADA system is known to use this attack.
3.3.2.3.2	Exploit Controler MODBUS registers Vulnerability	LEAF	Single-Threaded Attack	ModBus Registers based devices hacking needs very good programer skills.
3.3.3	Identify SCADA System Secondary Server IP Address	OR		
3.3.3.1	Scan for Banners in Secondary Server OS	LEAF	Single-Threaded Attack	
3.3.3.2	Probe TCP-IP Stack for OS Character Identification	LEAF	Single-Threaded Attack	
3.3.3.3	Determine Remote RTU Router MAC Address	OR		
3.3.3.3.1	Exploit AC 800 F Controler Vulnerability	LEAF	Single-Threaded Attack	
3.3.3.3.2	Exploit Controler MODBUS registers Vulnerability	LEAF	Single-Threaded Attack	ModBus Registers based devices hacking needs very good programer skills.
3.3.4	Identify SCADA System WEB Server IP Address	OR		
3.3.4.1	Exploit DoS Vulnerabilities of WEB Server OS	LEAF	Multi-Threaded Attack	In theory there should separate sub trees for each protocol riding on top of IP (TCP, MDP).
3.3.4.2	Web Server Vulnerabilities	OR		
3.3.4.2.1	Access Sensitive LAN Resources Directly	LEAF	Single-Threaded Attack	Only one or two familiar persons with SCADA system is known to use this attack.
3.3.4.2.2	Access Data from Previleged Accounts	LEAF	Single-Threaded Attack	Only one or two familiar persons with SCADA system is known to use this attack.
3.3.5	Identify SCADA System Application Server IP Address	OR		
3.3.5.1	Exploit DoS Vulnerabilities in Application Server OS	LEAF	Multi-Threaded Attack	Control or to modify the SCADA application software to gain control of Application Server
3.3.5.2	Application Software Vulnerabilities in App. Server	LEAF	Multi-Threaded Attack	Control or to modify the SCADA application software to gain control of Application Server

5. OFFSHORE OIL AND GAS PROCESS COMPLEX ATTACK TREE MODELING

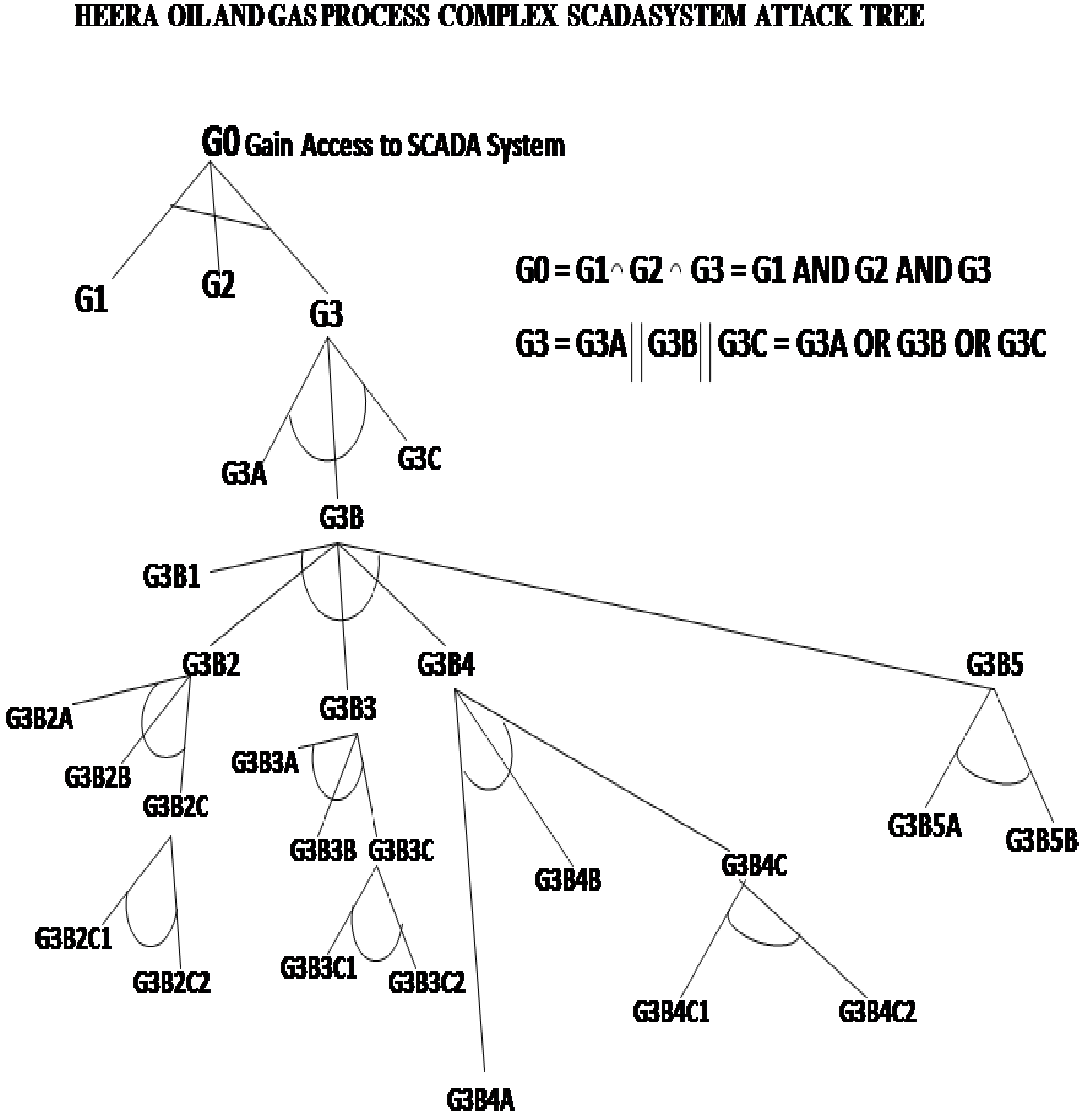

HEERA OILAND GAS PROCESS COMPLEX SCADASYSTEM ATTACK TREE
G0 Gain Access to SCADA System
G1
G2
G3
G0 = G1 ∧ G2 ∧ G3 = G1 AND G2 AND G3
G3 = G3A || G3B || G3C = G3A OR G3B OR G3C
G3A
G3C
G3B
G3B1
G3B2
G3B3
G3B4
G3B5
G3B2A
G3B2B
G3B2C
G3B3A
G3B3B
G3B3C
G3B5A
G3B5B
G3B4B
G3B4C
G3B2C1
G3B2C2
G3B3C1
G3B3C2
G3B4C1
G3B4C2
G3B4A

Fig 4: Offshore Oil and Gas Process Complex SCADA System Attack Tree

Total Nodes in Heera Oil and Gas Process Complex SCADA System Attack Tree

G0 = <AND> Gain Access to Heera Oil and Gas Process Complex (HPC) SCADA System

G1 = Identify Heera Process Complex Domain Name Service (DNS)

G2 = Interrogate Heera Process Complex DNS

G3 = <OR> Identify Heera Process Complex SCADA System Fire Wall

G3A = Port SCAN HPC SCADA System Fire Wall

G3B = Trace Route to HPC SCADA System Fire Wall

G3C = <OR> Determine SCADA System Fire Wall Access Control

G3B1 = Determine MAC Address of HPC SCADA Router

G3B2 = <OR> Identify SCADA System Primary Server IP-Address

G3B2A = SCAN for Banners in Primary Server Operating System

G3B2B = Probe TCP-IP Stack for Operating System Character Identification

G3B2C = <OR> Determine Remote location RTU Router MAC Address

G3B2C1 = Exploit AC800F Controller Vulnerabilities

G3B2C2 = Exploit Controller MODBUS Vulnerabilities

G3B3 = <OR> Identify SCADA System Secondary Server IP-Address

G3B3A = SCAN for banners in Secondary Server Operating System

G3B3B = Probe TCP-IP Stack for Operating System Character Identification

G3B3C = <OR> Determine Remote location RTU Router MAC Address

G3B3C1 = Exploit AC800F Controller Vulnerabilities

G3B3C2 = Exploit Controller MODBUS Vulnerabilities

G3B4 = <OR> Identify SCADA System WEB Server IP-Address

G3B4A = DoS Vulnerabilities of WEB Server

G3B4B = <OR> WEB Server Vulnerabilities

G3B4C1 = Access Sensitive LAN Resources

G3B4C2 = Access Data from Privileged Accounts

G3B5 = <OR> Identify SCADA System Application Server IP-Address

G3B5A = DoS Vulnerabilities in SCADA System Application Server

G3B5B = Application Server Application Software Vulnerabilities

6. RESULTS AND DISCUSSION

Tier-1 SCADA System at Offshore Oil and Gas Process Complex Attack Tree Generation Flow Chart developed and also Attack Trees designed and constructed. Detailed list of label, name, node type, node attack and node details are tabulated in a tabular form in table 1. The node gain access to Heera Process complex SCADA system is denoted by label ‘0’ and it is represented by AND-gate. Any able person can carry this attack. Labels 1and 2 denote - Identify and Interrogate Heera Process Complex DNS represented by leafy nodes. They are subjected to single threaded attacks and requires a PC with internet connection. Label 3 denotes Identify Heera Process complex Fire wall represented by OR-gate. Port SCAN and Trace Route to Heera Process complex SCADA system Fire walls are leafy nodes. Attacks are multi threaded. In this particular case entering SCADA network requires tunnel and break through the hardware fire wall. SCADA system fire wall access control node is represented by OR-gate. The SCADA system routers MAC address determination represented by leafy node. Identifying IP-address of Primary Server represented by OR-gate. Scanning Primary server for banners is denoted by leafy node. Node attack is single threaded attack. Probing TCP-IP stack for OS character identification is also leaf node but it requires multi threaded attacks. Determination of remote oil and gas platform router MAC address is denoted by OR-gate. Replicating worm to find router MAC address necessarily requires skilled network engineer. Exploiting AC 800F RTU Controller and RTU Modbus registers are leaf nodes. Only known persons about SCADA system can mount this type of attack. These attacks are single threaded. As the SCADA system is provided with redundancy, Secondary Server also follows same attacks routine in attack tree model. Web-Server in SCADA network is meant for Tier-2 connectivity. Web-Server IP-Address determination is denoted by OR-gate. Exploitation of DoS vulnerabilities of Web Server OS is a leaf node. Node attack type is multi threaded and there should be separate sub trees for each protocol riding on top of IP (TCP, MDP). Web-Server vulnerabilities is node denoted by OR-gate. Access sensitive LAN resources directly and access data from privileged accounts are two leaf nodes under this OR-gate. The Identification SCADA system Application Server IP-Address is depicted by OR-gate. Exploiting DoS vulnerabilities in application server OS and application software vulnerabilities are leaf nodes under above OR-gate. To gain control over application server and effecting its functions are multi threaded attacks. Total number of nodes in process complex SCADA system attack tree determined to be 28. It means there are twenty seven vulnerabilities will aid for intruder in taking complete control over the SCADA system at process complex.

Conclusion: The present work limited to designing Attack Tree for Tier-1 SCADA system comprising of four severs, router, and fire wall at offshore oil and gas process complex and remote platform RTU controller and Modbus registers. The process complex SCADA system is implemented in Tier structure and is incorporated into corporate LAN. Since it is accessible through corporate LAN inherent dangers of cyber threats exist to the SCADA network. Keeping this point in mind the Attack Tree model conceived with an idea that SCADA system may be exposed to the various network threats. It is small beginning and effort to analyze the SCADA system by visualizing and anticipating common threats and vulnerabilities. Taking into consideration of above modeling, attention is drawn to following points will help in reducing intrusions into SCADA system network. External connections outside the process complex are in secure and if possible may be encrypted. In SCADA network important Gateway devices like fire walls, routers, switches, communicating with beyond process complex devices susceptible to cyber attacks these devices should be hardened. Corporate intrusion detection system deployed on Offshore Oil and Gas Process Complex SCADA system network helping to mitigate cyber threats.

7. REFERENCES

[1] B. Schneier, “Modeling security threats,” *Dr. Dobb’s Journal*, 1999.

[2] Phillps C, Swiler L P, “A Graph-based System for Network Vulnerability Analysis”, *Proceedings of the 1998 workshop on new security paradigms*, VA, USA: ACM Press, pp. 71-79, 1998.

[3] Meadows C, “ A Representation of protocol attacks for risk assessment”, Network Threats, DIMACS series in Discrete Mathematics and Theoretical Computer Science, Vol 38, R.N. Wright and P.G. Neumann editors, American Mathematical Society, PP 1-10.

[4] J, Ramakrishman C, Skar R, “Model-based Vulnerability Analysis of Computer Systems”, *Proceedings of the 2nd International Workshop on Verification*, Pisa, Italy: Model Checking and Abstract Interpretation Press, pp. 1-81, 1998.

[5] Ammann P, Pamuls J, Ritchev R, “A Host Based Approach to Network Attack Chaining Analysis”, *Proceedings of the 21st Annual Computer Security Applications Conference*, Tucson, Arizona, USA: IEEE Computer Society Press, pp. 72-84, 2005

[6] N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic security risk management using Bayesian attack graphs,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 61–74, 2012.

[7] B. Ivanc and T. Klobucar, “Critical infrastructure attack modeling,” *Elektrotehniski Vestnik*, vol. 79, no. 4, pp. 193–196, 2012.

[8] SecurI Tree**,** Amaneza Tech Limited, A Quick Tour of Attack Tree Based Risk Analysis using SecurI Tree, Technical report, 2002.

[9] Alexander Opel, “Design and Implementation of a Support Tool for Attack Trees, 2005.

[10] TANAT Threat ANd Attack Tree Modeling Plus Simulation, 2004, http://www13.informatik.tu-muenchen.de:8080/tanat.

[11] Stefan Einarsson and Marvin Rausand “An Approach to Vulnerability Analysis of complex industrial systems, Risk Analysis, 18(5): 535-545, 1998.

[12] Jan Stefan and Markus Schumacher, “Collaborative attack modeling in Proc.SAC 2002, pages 253-259, ACM 2002.

[13] J.P.Mcdermott, “Attack net penetration testing in Proc.2000, workshop on security paradigm, pages 15-20, ACM 2001.

[14] Mauw S., Oostdijk M.(2006)Foundations of Attack Trees. In: Won D.H., Kim S.(eds) Information Security and Cryptology – ICISC 2005. ICISC 2005. Lecture notes in Computer Science, vol 3935. Springer, Berlin, Heidelberg.