Multi Tree View of Complex Attack – Stuxnet

Shivani Mishra[1], Krishna Kant[2], and R.S. Yadav[3]

[1] Research Scholar, CSED, Motilal Nehru National Institute of Technology, Allahabad, Uttar Pradesh, India
[2] Professor, Computer Engineering and Applications Department, GLA University, Mathura, India
[3] Professor, CSED, Motilal Nehru National Institute of Technology, Allahabad, Uttar Pradesh, India
shivanialld@gmail.com, krishna.kant@gla.ac.in, rsy@mnnit.ac.in

Abstract. Stuxnet attack on critical infrastructures is considered as paradigm shift in malware attack approach. The complexity and sophistication involved in this attack make it unique. Attacking approach of the malware, on control infrastructures, is a motivation for academic research. This paper describes the application of the Attack Tree methodology to analyze Stuxnet attack on SCADA system. Root node of the Attack Tree represents the major goal of an attacker and branches represent sub goals. The authors have identified six major goals to penetrate SCADA system, and then have built Attack Trees which demonstrate step by step activity to achieve these goals and sub goals. For each such sub goal, we have found several common categories of attacks which make Stuxnet attack successful and are used to analyze those components of control infrastructure which are susceptible to attacks.

Keywords: Malware, Stuxnet, SCADA , Control infrastructures, Attack Trees, Attack Goal, Attack Sub Goal.

1 Introduction

Nowadays, sustained cyber attacks against critical infrastructure have been escalated to an alarming situation. They are causing havocs to digital installations with a very sophisticated manner and enormous frequency. A complex computer worm, discovered in June 2010, effectively disabled Iran's nuclear program for more than a year. It happened even when their nuclear facilities were highly secured, located underground physically and electromagnetically isolated from insecure networks known as Air Gapped from the Internet (AGI) [1].

The recent findings, as documented in reports published by Symantec [2], ICS-CERT [3], and Eset [4] indicate that worm was propagated to ins and outs of the facility from universal serial bus, USB, using thumb drive technology through AGI. The AGI was used as via media to allow worm to penetrate the SCADA system. The highly complex computer worm called Stuxnet was designed to spread until it found specific control system as its target. Investigating experts have opined that the worm, so used is the first weaponized virus [5] [6].

N. Meghanathan et al. (Eds.): Advances in Computing & Inform. Technology, AISC 176, pp. 171–188.
springerlink.com

In the present research paper, our focus is to analyze the notorious Stuxnet worm (WIN 32/Stuxnet) attack on SCADA system using the Attack Tree approach. Bruce Schenier is the one and the first researcher who introduced Attack Tree modeling to analyze attacks [7]. Early approaches to this problem through the Attack Tree modeling heavily relied upon

1. Categorization of attack sequences and modeling the path traced by the attacker to exploit the system [8].
2. Assuming all elementary attacks took place simultaneously, some researchers adopted parallel modeling, which consist of attack models parallel to the actual incidents so assumed [9].

In the context we assume, ab nitio, that the attacker had different attack alternatives, if some initiations fail to succeed, at least one would definitely succeed. In our work we propose detection oriented security modeling approach using Attack Trees for Stuxnet attack on SCADA system. In this track of security modeling evaluation process we first determine,

1. Goals and Sub Goals of an Attacker to penetrate the system
2. Vulnerabilities in the system
3. Common Category of attacks which enable Stuxnet to execute
4. Resources exploited by these attacks

The organization of the paper is as follows. Section 1 is the Introduction to Stuxnet attack scenario in critical SCADA systems. Section 2 gives motivational background for the present work. A brief review of the relevant work is made in Section 3. Section 4 presents the proposed work – Attack Tree structure for Stuxnet malware attack. Conclusions are drawn in Section 5.

2 Background

2.1 Introduction of SCADA Systems

The systems that control critical infrastructures are Industrial Control Systems (ICS). There are several types of control systems in it including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other smaller control systems such as Programmable Logic Controllers (PLC). Industries associated with critical infrastructure include power generation and distribution, oil and gasoline refining and distribution, water and waste systems, manufacturing, telecommunications, and banking infrastructures.

SCADA systems, an architectural block diagram of which is shown in Fig 1, consist of:

- One or more field data interface devices, usually Remote Terminal Unit (RTU), or PLCs, which interface to field sensing devices and local control switchboxes and valve actuators.
- A communications system used to transfer data between field data interface device and control units and the computers in the SCADA central host. The system can be radio, telephone, cable, satellite, etc., or any combination of these.

- A central host computer server or servers (Also known as SCADA Center, master station, or Master Terminal Unit (MTU)
- A collection of standard and/or custom software (Known as Human Machine Interface (HMI) software or Man Machine Interface (MMI) software) systems used to provide the SCADA central host and operator terminal application, support the communications system, and monitor and control remotely located field data interface devices

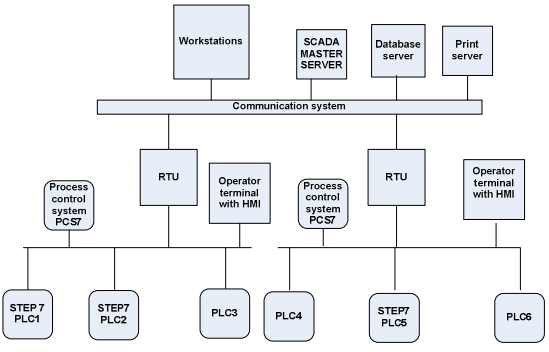

Fig. 1. Typical SCADA architecture

Software products typically used within a SCADA system are for the following purpose:

- **Central host computer operating system**: Software used to control the central host computer hardware. The software can be based on Windows, UNIX or other popular operating systems.
- **Operator terminal operating system**: Software used to control the central host computer hardware. The software is usually the same as the central host computer operating system. This software, along with that for the central host computer, contributes to the networking of the central host and the operator terminals.
- **Central host computer application**: Software that handles the transmission and reception of data to and from the RTUs and the central host. The software also provides the graphical user interface which offers site mimic screens, alarm pages, trend pages, and control functions.
- **Operator terminal application**: Application that enables users to access information available on the central host computer application. It is usually a subset of the software used on the central host computers.
- **Communications protocol drivers**: Software that is usually based within the central host and the RTUs, and is required to control the translation and interpretation of the data between ends of the communications links in the system. The protocol drivers prepare the data for use either at the field devices or the central host end of the system.

- **Communications network management software**: Software required to control the communications network and to allow them to be monitored for performance and failures.
- **RTU automation software**: Software that allows engineering staff to configure and maintain the application housed within the RTUs (or PLCs). Most often this includes the local automation application and data processing tasks that are performed within the RTU [10].

2.2 Stuxnet Attack on SCADA

Stuxnet is a computer worm, discovered in June 2010. It targets Siemens industrial software and equipment running on Microsoft Windows. It is the first discovered malware that spies on and subverts industrial systems, and the first to include a PLC root kit. The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens SCADA systems that are configured to control and monitor specific industrial processes. Stuxnet infects PLCs by subverting the Step-7 software application (SIMATIC Step7 is an integral component of the centralized Totally Integrated Automation Portal engineering framework) that is used to reprogram these devices [11].

Stuxnet worm is so intelligent that it makes itself neutral if Siemens software is not found on infected computers, Stuxnet contains code for a man-in-the-middle (MITM) attack through hooking that jukes industrial process control signals so as the infected system does not alarm due to this abnormal behavior. Such complexity is very unusual for malware. The attacking strategy of this malware can be divided in two parts, they are as follows-

1. Gain access on Windows operating system,
2. Disrupt Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows.

Windows infection

Stuxnet attack occurs on Windows systems using four zero-day attacks. A zero-day attack is exploitation of computer system software vulnerabilities that are not known to others. Initially it spreads using infected removable drives such as USB flash drives, and then uses other exploits and techniques such as peer-to-peer RPC to infect and update other computers inside private networks that are not directly connected to the Internet.

SIMATIC WinCC is a supervisory control and data acquisition system from Siemens. It can be used in combination with Siemens PCS 7 and Teleperm, a process control system. WinCC is written for Microsoft Windows operating system. WinCC uses Microsoft SQL Server for logging and comes with a VBScript and ANSI C application programming interface. WinCC and PCS 7 are the first SCADA systems which were targeted by malware to subvert control system [12].

3 Related Work

The complex infrastructure of SCADA systems provides great capabilities for operation, control and availability of resources, simultaneously it also increases security risk due to cyber related vulnerabilities. Disruption, information leakage, malfunctioning of system process can cause havoc in the system which in turn causes negative financial impact for the system. Because of critical nature of these systems, they are now targets for adversaries.

Digital security for critical infrastructure requires extensive research methodology for securing control system rather than focusing only on securing IT system associated with SCADA systems. In [13], Manimanran et al. (2010) has proposed SCADA security framework with the following four major components. They are Real time monitoring, Anomaly detection, Impact Analysis and Mitigation strategies.

The Attack tree modeling is used for impact analysis. System-, scenario-, and leaf-level vulnerabilities are discovered by identifying system's adversary objectives. The leaf vulnerability involves port auditing or password strength evaluation which is a measure of intrusion in a system. The approach used in this paper is extensive and can be applied for evaluation of different parameters of security like confidentiality, integrity, availability and authentication so that possibility of attack related to parameters such as eavesdropping, modification, malware attacks, like, virus, worm, Trojan horse, bypassing controls can be measured and countermeasures are predetermined.Malware attacks like Stuxnet is considered as paradigm shift in critical infrastructure threats. Unlike most malwares, Stuxnet has great capabilities to attack in depth for controlling physical machinery. At the same time the sophistication is found in Stuxnet programming which is considered as "a new class and dimension of malware" [14] [15]. The worm's code was written in multiple programming languages. Research has also speculated that Stuxnet was professionally developed and would have required access to SCADA hardware for testing. Stuxnet employs multi vector approach by exploiting four zero-day vulnerabilities, out of which two were privilege escalation, and remaining were printer spooler flaw & USB flash drive [16]. Stuxnet is considered as epochal because of its ability to infiltrate networks, find control system of supervisory and data acquisition industry and reprogram the hardware control system. A nuclear facility was attacked by Stuxnet [17].

The sophistication and capability to penetrate the system invisibly make the Stuxnet worm attack as complex attack. A complex attack can be described as

Multi Agent: For Stuxnet Attack, threat agent can be one or many who want to sabotage the facility of SCADA system, at the same time threat agent can take one or more actions for the successful completion of an attack.

Multi Phase: Stuxnet attack has several attack stage. Specifically these stages are exploits at different junctures.

Multi Pace: Stuxnet choice of target is very specific. For successful attack it involves multiple *intrusion* activities in a SCADA system to reach the intended target.

An Attack Tree approach to analyze Stuxnet worm activity inside SCADA systems is the main contribution of our work. In the next section a brief description of Attack Tree and Stuxnet attack approach visualization through Attack Tree is mentioned

4 Attack Tree Approach for Problem Solving

Attack Trees were introduced by B. Schneier, as a way of formally analyzing the security of systems. Since this methodology is efficient to model the behavior of an attacker while attacking on a system, security researchers are gaining interest to use this technique as a tool for evaluation of different aspects of security[18] [19].

Basically an Attack Tree approach is systematic categorization of different ways to attack on a system. In this structure a root node represents main goal of an attacker and intermediate nodes are representative of sub goals to achieve main goal. Branches of an Attack Tree represent different paths to achieve a goal and are termed as sub goals. Leaf nodes represent attack as a compromised state of system as an event and moving upward in a tree gives the ways to reach to the sub goals and finally to the main goal. Attack sub goals and Attack main goals are also connected with AND/OR Nodes. Tree traversal is from left to right and is shown by Ordered –AND nodes and Ordered –OR nodes (O-AND/OR). It is necessary to mention here that all nodes of a Tree may or may not have precedence order (O). An attack goal is successfully achieved when all of its AND children or at least one of its OR children are accomplished. This is same for all sub goals down to leaves of the tree [20].

We have followed various reports published by Symantec, and Eset, on Stuxnet attack, for analyzing Stuxnet attack strategy through Attack Tree. This attacking strategy is divided in six major goals and is represented in Fig 2.

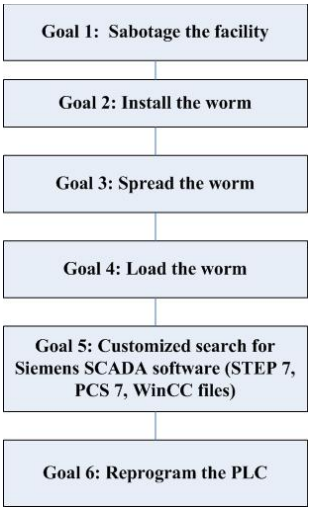

Fig. 2. Attack strategy of Stuxnet

Attack Goal 1: Sabotage the Facility

The main goal of an attacker was to sabotage the SCADA system. For this an attacker can target SCADA center system access, communication system, or disrupt field data interface. A central host computer server and HMI software's on host computers constitute SCADA central systems. SCADA central host computer servers are Master server, database servers, print servers and network server etc. A Human Machine interface (HMI) i.e. application software installed on central host computer presents process data to human operator. To disrupt HMI an attacker can gain access on central host computer, Operator terminal O.S, central host computer applications, communication protocol drivers, Operator terminal applications, communication network management software & RTU Automation systems. To disrupt communication systems an attacker can disable transmission media or exploit any vulnerability in communication media. Lastly an attacker can destruct field data interface by modifying the code written for PLC's and corrupt Remote telemetry unit's interfaces. In case of Stuxnet the main target of an attacker is to reprogram Industrial control system by modifying code on Programmable logic controllers (PLC's), specifically for Siemens SIMATIC/WINCC PCS7 software.

The Attack Tree, shown in Fig 3 and Fig 4, outlines the methods of gaining access to the SCADA system. The intention is to determine all the possible goals of an attacker to deploy Stuxnet in SCADA system.

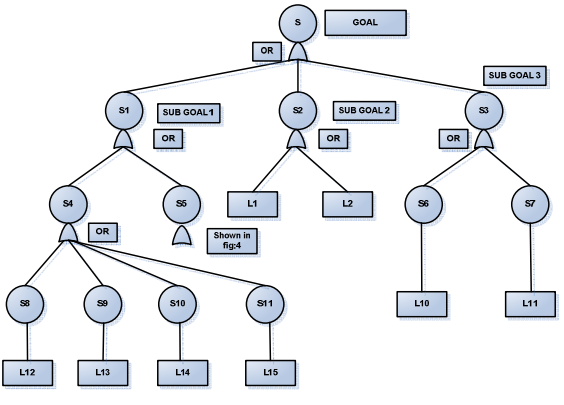

Fig. 3. Methods to sabotage the SCADA system

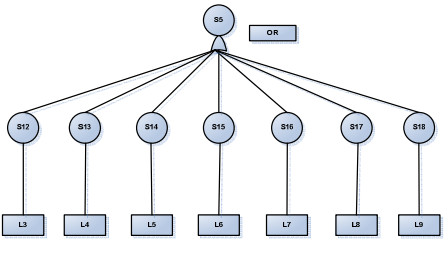

Fig. 4. Methods to Disrupt HMI

Attack Goal 1: Sabotage the SCADA System (S)
Sub Goal 1: Gain SCADA center system access (S1) OR
1.1. Gain access to central host computer servers (S4) OR
1.1.1. Compromise SCADA Master server (S8) OR
1.1.2. Compromise SCADA Master Database server (S9)OR
1.1.3. Compromise SCADA Master print server (S10) OR
1.1.4. Compromise SCADA Master network server (S11)
1.2. Disrupt HMI (S/w products used within SCADA) (S5) OR
1.2.1. Gain control on central host computer O.S (S12, L3) OR
1.2.2. Gain control on Operator terminal O.S. (S13, L4) OR
1.2.3. Gain control on central host computer applications. (S14, L5) OR
1.2.4. Disrupt communication protocol drivers (S15, L6) OR
1.2.5. Gain control on Operator terminal applications (S16, L7) OR
1.2.6. Disrupt communication network management software (S17,L8) OR
1.2.7. Subvert RTU Automation (S18,L9)
Sub Goal 2: Disrupt communication system (S2) OR
2.1. Disable Transmission media (L1)
2.2. Exploit Vulnerabilities in SCADA communication protocols (L2)
Sub Goal 3: Disrupt field data interface (S3)
3.1 Disrupt PLC (S6) OR
3.1.1Corrupt software at operator terminal (SIMATICPCS7) (L10)
3.2 Disrupt RTU (S7)
3.3 Subvert RTU Automation software (Modular controllers SIMATIC S7) (L11)

Analysis

On analyzing Attack Tree we have derived three sub goals a) Gain access to SCADA center system, b) Disrupt communication system and PLC, c) Disrupt field data interface, aimed by attackers for deploying Stuxnet malware in SCADA systems.

We have also found several attack methods used for achieving Goal1 of stuxnet. Critical resources which were targeted by these attacks are also listed. A One-to-Many relationship is characterized between attacks and resources, because for an attack, one or more resources can be exploited.

Attacks={MITM, Denial of service against Network, Privilege escalation, Unauthorized access, Flooding attack for PLC's, Root kit Attack, Buffer overflow Attack, Export hooking to gather PLC information, Resource Exhaustion}

Resources={Hardware servers, Print servers, Operating system, Database software, Automation and control Software, Communication channels, Communication protocols, Remote Terminal units, PLC software, Process control system}

Descriptions are provided for the following generic attack types.

1. MITM Attack

Man in the middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them. The attacker must be able to intercept all messages going between the two victims and inject new ones. A man-in-the-middle attack succeeds only when the attacker impersonates each endpoint to the satisfaction of the other; it is an attack on mutual authentication.

The two compromised certificates from Jimicron and Realtek enabled this malware to execute user mode and kernel mode root kit under Windows, it is by-passing authentication mechanism. Data communication between a PLC

and an HMI was targeted through MITM attack. Stuxnet caused modified data to be reported at HMI, which lead to the undesirable events for operator. At this juncture control systems started behaving abnormally, which resulted in further sabotage.

2. **Denial of Service Against Network**

   A Denial of service (DOS) attack is an attempt by attacker to prevent intended users from using the service by consuming network bandwidth, disrupting connections between machines.

   In case of Stuxnet attack an attacker has used printer and network connections to spread the information. The vulnerability exploited is MS10-061, The Vulnerability in printer spooler service (CVE-2010-2729) could allow remote code execution, if a system shares a printer over the network. Attackers have found a way to exploit MS08-67 vulnerability, an old RPC vulnerability in Windows server service for peer-to-peer servers to initialize DOS attacks. This form of attack basically enabled to get Stuxnet version, injection of specific module and send the malware through peer to peer network. In this way Stuxnet were identified, communicated and updated to each other.

3. **Resource Exhaustion**

   Resource exhaustion is a kind of denial of service attack, in which particular resource is consumed so that it is not available at the time it is required or system is not responding for legitimate requests. Vulnerabilities found in system architecture, protocol services, are subject to resource exhaustion attack.

   In case of Stuxnet attack on control infrastructure, different servers, communication bandwidth, vulnerabilities, found in MODBUS protocol and some application programs like Siemens S7 programs were targeted for resource exhaustion.

4. **Sniffing**

   Sniffing is a kind of passive eavesdropping. The Stuxnet code contains Trojan to sniff data to send and receive information from remote systems. The vulnerability MS10-046 in Windows shell allowed Remote code execution. Another vulnerability MS08-67 in server service could allow remote code execution based on sniffed information.

5. **Privilege Escalation**

   The Privilege Escalation via keyboard layout file (MS10-073) and via task scheduler, were seen in Stuxnet attack for gaining access to resources. These vulnerabilities were exploited to get permission from normal user level to system level permissions. MS08-67 vulnerability in server service allows remote code execution and MS10-073 vulnerability in Windows kernel mode drivers could allow elevation of privileges. Both vulnerabilities are responsible for privilege escalation by Stuxnet.

6. **Unauthorized Access**

   Unauthorized access to a *SCADA* network through an unprotected USB port is the method used to launch the Stuxnet worm. The MS10-046 Windows shortcut vulnerability allowed unauthorized access to spread via removable drives even if auto run was disabled.

7. **Flooding Attack for PLCs**
   Flooding attacks are also DOS attacks in which some specific ports are flooded with packets. An easy way to perform DOS attack on PLCs could be flooding PLC with data or command. Once the Stuxnet worm located in a targeted SCADA system uploads its own program into PLCs to control the automation process and finally flood the PLC with command, causing damage to resources.
8. **Root Kit Attack**
   The Stuxnet attack is a kind of attack which includes PLC root kit. This malware has both user mode and kernel mode root kit capability under Windows. Thus modification in code remains undetected for long period of time.
9. **Buffer Overflow Attack**
   Buffer overflow attacks take advantage of known vulnerabilities within operating system and applications. A buffer overflow occurs when an application receives unexpected data. Stuxnet used malicious code injection in Siemens system and caused buffer overflow attack.
10. **Export Hooking to Gather PLC Information**
    API hooking is a technique used to intercept and alter the command or functions behavior of operating system or other application software. Basically a code has written (termed as hook) to intercept function calls. Stuxnet hooked Ntdll.dll file to monitor for requests to load specially crafted file names [21].

An evaluation table has been established which demonstrates the severity of each attack, i.e. its likelihood of occurrence while achieving a sub goal. The assessment is qualitatively, and on ordinal scale let us assume severity is rated as "High", "Medium", and "Low" and relative numeric scale is 9 , 7 , 5 respectively."High" level of an attack manifests that an adversary uses this category to its optimum precision and concerned application or resources need to be addressed significantly. Medium level attacks need to be addressed with less urgency depending upon how much effort and cost is required to provide countermeasure to stop the attack and low level of attack means at earlier stage it was high, but at present stage it causes to create a path for another attack.

Table 1. Attack severity for Goal 1

Attack	Severity for sub goal1		Severity for sub goal2		Severity for sub goal3	
	Level	Scale	Level	Scale	Level	Scale
MITM Attack	High	9	Medium	7	Low	5
DOS	Medium	7	High	9	High	9
Sniffing	Medium	7	Low	5	Medium	7
Privilege escalation	High	9	High	9	Medium	7
Unauthorized access	High	9	low	5	Medium	7
Flooding attack(PLC)	High	9	Low	5	High	9
Rootkit Attack	High	9	Low	5	High	9
Bufferoverflow Attack	High	9	Low	5	Low	5
Export hooking	Medium	7	Low	5	High	9
Resource Exhaustion	Medium	7	High	9	High	9

Folowing is a graph plot to quickly analyze the above facts.

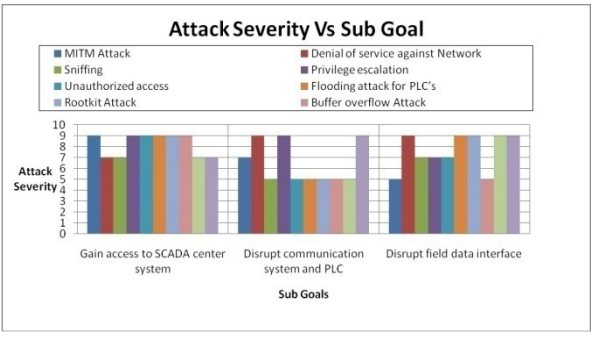

Fig. 5. Sub Goals and Attacks for achieving Goal 1

Attack Goal 2: Install the worm

Stuxnet has a complex architecture. The heart of Stuxnet consists of a large ".dll" file that contains many different exports and resources. Initialization of main installation of malware in the system starts with export 16. Export 16 first checks the value NTVM trace in registry. If the value is 19790509 it confirms existence of threat. This strategy was used to confirm whether Stuxnet is existing or not. After ensuring this, Stuxnet disables firewall settings to start installation procedure by dropping required files in Windows directory. Following Attack Tree demonstrates the procedure. All these activities are possible only when an attacker gains system level permission. Privilege escalation, unauthorized access, a form of MITM attack and root kit attack is seen at this juncture.

Attack Goal 2: Install Stuxnet O-OR
Sub goal 1: Begin main Installation (Invoke Export function 16#) O-OR
1.1. Check for NTVDMTRACE AND
1.2. Check for value 19790509
Sub goal 2: Write into Windows directory
2.1. Modify Windows firewall settings O-OR
2.2. Disable the Windows firewall

Analysis: For installing worm, the sub goal a) Begin main Installation (Invoke Export function 16#) and b) Write into Windows directory, have to be achieved. Possible attacks and exploited resources are as follows.
Attacks = {MITM, Privilege escalation, Unauthorized access, Root kit Attack}
Resources = {Hardware servers, Operating system, Database software, Automation and control Software, Communication and control Software}
Here we are showing all categories of attack because severity of some attacks are low but favors another category of attack for its successful completion.

Table 2. Attack severity for Goal 2

Attack	Severity for sub goal1		Severity for sub goal2	
	Level	Scale	Level	Scale
MITM Attack	High	9	Medium	7
DOS	Low	5	Low	5
Sniffing	Medium	7	Medium	7
Privilege escalation	High	9	High	9
Unauthorized access	High	9	Medium	7
Flooding attack (PLC)	Low	5	Low	5
Rootkit Attack	Medium	7	High	9
Buffer Overflow	Low	5	Low	5
Export hooking	Low	5	low	5
Resource Exhaustion	Low	5	Low	5

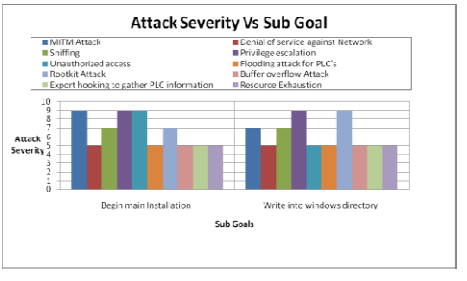

Fig. 6. Sub Goals and Attacks for achieving Goal 2

Attack Goal 3: Spread the worm

Stuxnet propagates by infecting removable drives and also by copying itself over the network using a variety of means. In addition, Stuxnet has the ability to copy itself into Step 7 projects using a technique that causes Stuxnet to auto-execute on opening of the project.

Attack Goal 3: Spread the worm
Sub goal 1: USB Drive infection OR
- 1.1. Spread via Exploiting .LNK vulnerability (CVE-2010-2568) AND
- 1.2. Stuxnet verify it is running under services.exe AND
  - 1.2.1. Create a file ~ WTR412.tmp O-AND
  - 1.2.2. Create a file ~ WTR4141.tmp
  - 1.2.3. Create shortcut to .lnk
  - 1.2.4. Create a copy of shortcut to .lnk
  - 1.2.5. Create a copy of copy of shortcut to .lnk
  - 1.2.6. Create a copy of copy of copy of shortcut to .lnk
  - 1.2.7. Check for versions of Windows
  - 1.2.8. Create a hidden window and wait for USB to be inserted
- 1.3. Use Export 19
  - 1.3.1. Copying Routine

Sub goal 2: Spread Via peer to peer communication
Sub goal 3: Spread via Network share

Analysis: Spreading of the worm was seen in three ways, the sub goal a) USB Drive infection b) Spread via peer to Peer communication and c) Spread via Network share. Possible attacks and resources are as follows.

Attacks = {MITM, Denial of service against Network, Privilege escalation, Unauthorized access, Root kit Attack, Export hooking to gather PLC information}
Resources = {Hardware servers, Print servers, Operating system, Database software, Automation and control Software, Communication channels, Communication protocols, Remote Terminal units, PLC software, Process control system}

Table 3. Attack severity for Goal 3

Attack	Severity for sub goal1		Severity for sub goal2		Severity for sub goal3	
	Level	Scale	Level	Scale	Level	Scale
MITM Attack	High	9	High	9	High	9
DOS	Medium	7	High	9	High	9
Sniffing	Low	5	Low	5	Medium	7
Privilege escalation	High	9	Medium	7	Medium	7
Unauthorized access	High	9	Medium	7	Medium	7
Flooding Attack(PLC)	Low	5	Low	5	Low	5
Root kit Attack	Medium	7	Low	5	Low	5
Buffer overflow	Low	5	Low	5	Low	5
Export hooking	High	9	Medium	7	High	9
Resource Exhaustion	Low	5	Low	5	Low	5

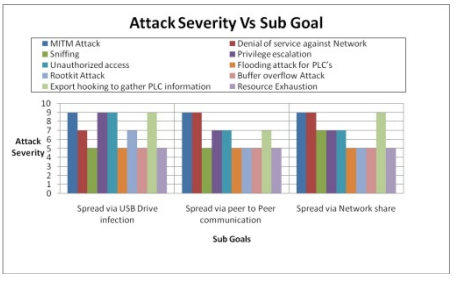

Fig. 7. Sub Goals and Attacks for achieving Goal 3

Attack Goal 4: Load the worm

At this juncture the main objective of attacker was execution of Stuxnet malware every time whenever infected system boots up. This task was performed by Mrxcls.sys driver. The goal of driver was to inject and execute copies of Stuxnet in to specific processes. The code snippet written for this driver has user mode and kernel mode privileges.

Attack Goal 4: Load the worm
Sub goal 1: Load Stuxnet module into a process by Mrxcls.sys driver O-AND
1.1 Get process address
Sub goal 2: Inject Stuxnet module into the process in kernel mode and user mode
2.1. Allocate memory AND
2.2. Execute Stuxnet.dll AND
2.2.1. Call exports AND
2.2.2. Call resources
2.3. Create MZ and PE files.

Analysis: Sub goals discovered at this stage are a) Load Stuxnet module into a process by Mrxcls.sys driver, b) Inject Stuxnet module into the process in kernel mode and user mode, for loading Stuxnet malware in SCADA systems.
Attacks = {MITM, Privilege escalation, Unauthorized access, Flooding attack for PLC's, Root kit Attack, Export hooking to gather PLC information, Resource Exhaustion}
Resources = {Hardware servers, Print servers, Operating system, Database, Remote Terminal units, PLC software}

Table 4. Attack severity for Goal 4

Attack	Severity for sub goal1		Severity for sub goal2	
	Level	Scale	Level	Scale
MITM Attack	Medium	7	Medium	7
DOS	Low	5	Low	5
Sniffing	Medium	7	Medium	7
Privilege escalation	High	9	High	9
Unauthorized access	High	9	Medium	7
Flooding attack (PLC)	Low	5	low	5
Rootkit Attack	Medium	7	High	9
Buffer overflow	Low	5	Medium	7
Export hooking	High	9	High	9
Resource Exhaustion	Low	5	Medium	7

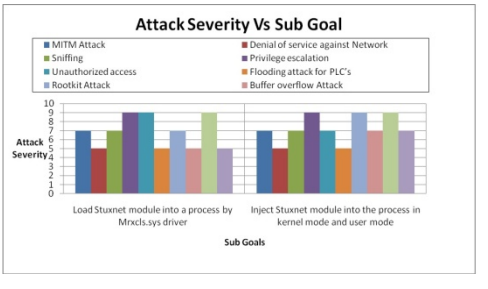

Fig. 8. Sub Goals and Attacks for achieving Goal 4

Attack Goal 5: Searching for step 7 project files

WinCC Simatic manager, used to manage a WinCC/Step7 project. Stuxnet monitor step7 projects (.S7P files). Hooking method is used to open specific APIs from project files inside the s7tgtopx.exe process. Following is Attack Tree representation of searching and infecting step7 project files.

Attack Goal 5: Search for step 7 project files
Sub goal 1: Search for .S7P file extensions OR
1.1. Create Following files O-AND
1.1.1. xutils\listen\xr000000.mdx O-AND
1.1.2. xutils\links\s7p00001.dbf
1.1.3. xutils\listen\s7000001.mdx

1.2. Scan Sub folders Under h0msave7 O-AND
1.2.1. Drop Resource 202
1.3. Modify step 7 project files
1.3.1. Modified step7 data files
Sub goal 2: Search for .mcp file extensions and infect project and WINCC database OR
2.1. Create Following File O-AND
2.1.1. GracS\cc_alg.sav O-AND
2.1.2. GracS\db_log.sav O-AND
2.1.3. GracS\cc_alg.sav xutils\listen\s7000001.mdx
2.2. Scan Sub folder GracS
2.2.1. Dropped a copy of resource 203
Sub goal 3: Search for .tmp file extensions
3.1 Validate file name OR
3.2 Examined contents of the file OR
3.3 Update for newer versions

Analysis: On analyzing Attack Tree we have derived three sub goals a) Search for .S7P file extensions, b) Search for .mcp file extensions and infect project and WINCC database, and c) Search for .tmp file extensions, aimed by attackers for searching the targeted step7 project files in SCADA systems.
Attacks = same as mentioned for Goal 4 and
Resources={Hardware servers, Operating system, Database software, Automation and control Software, Communication channels, Remote Terminal units, PLC software, Process control system}

Table 5. Attack severity for Goal 5

Attack	Severity for sub goal1		Severity for sub goal2		Severity for sub goal3	
	Level	Scale	Level	Scale	Level	Scale
MITM Attack	Medium	7	Medium	7	Medium	7
DOS	Low	5	Low	5	Low	5
Sniffing	Medium	7	Medium	7	Medium	7
Privilege escalation	High	9	High	9	Medium	7
Unauthorized access	Medium	7	Medium	7	Low	5
Flooding attack (PLC)	Medium	7	Medium	7	Low	5
Rootkit Attack	Medium	7	Medium	7	Low	5
Buffer overflow	Medium	7	Low	5	High	9
Export hooking	High	9	High	9	High	9
Resource Exhaustion	High	9	Medium	7	Low	5

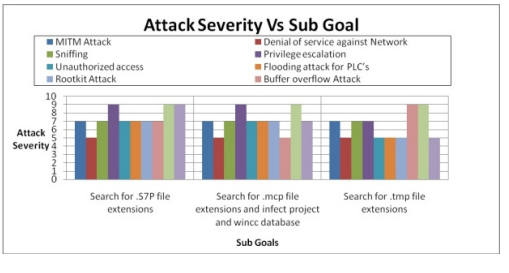

Fig. 9. Sub Goals and Attacks for achieving Goal 5

Attack Goal 6: Modify PLC code

The end goal of Stuxnet is to infect specific types of Simatic PLC devices. PLC devices are loaded with blocks of code and data written using a variety of languages, such as STL or SCL. The compiled code is an assembly called MC7. These blocks are then run by the PLC, in order to execute, control, and monitor an industrial process.

Resource 208 is dropped by export #17 and is a malicious replacement for Simatic's s7otbxdx.dll file. The original s7otbxdx.dll is responsible for handling PLC block exchange between the programming device (i.e., a computer running a Simatic manager on Windows) and the PLC. By replacing this .dll file with its own, Stuxnet is able to perform the following actions:

1. Monitor PLC blocks being written to and read from the PLC.
2. Infect a PLC by inserting its own blocks and replacing or infecting existing blocks.
3. Mask the fact that a PLC is infected.

Attack Goal 6: Modify PLC code
Sub goal 1: Monitor PLC Blocks O-AND
1.1. Target WinCC/Step7 and s70tbxdx.dll
Sub goal 2: Infect PLC Blocks O-AND
2.1. Rename s70tbxdx.dll to s70txsx.dll O-AND
2.2. Replace the original dll with its original malicious code. O-AND
2.2.1. Intercept hooking process O-AND
2.2.2. Start malicious thread O-AND
2.2.2.1. Run an infection routine in every 15 seconds O-AND
2.2.2.2. Infect CPU's O-AND
2.2.2.3. Regularly query PLC for specific block O-AND
2.2.2.4. Customize code block O-AND
Sub goal 3: Mask PLC infection (PLC Root kit)
0.1. Monitor and read requests O-AND
0.1.1. Read requests for its own malicious block OR
0.1.2. Read requests for infected blocks OB1, OB35, DP-RECV
0.2. Intercept the code O-AND
0.2.1. Write requests that could overwrite Stuxnet's own code
0.3. Modify code
0.3.1.Modify requests to ensure new version of code block are infected OAND
0.3.2.Read block of code O-AND
0.3.3.Delete block of code

Analysis: At this juncture sub goals are a) Monitor PLC Blocks, b) Infect PLC Blocks, c) Mask PLC infection, for modifying PLC's in SCADA systems.
Attacks = {MITM, Privilege escalation, Unauthorized access, Flooding attack for PLC's, Root kit Attack, Buffer overflow Attack, Export hooking to gather PLC information, Resource Exhaustion}
Resources = {Operating system, Database software, Automation and control Software, Remote Terminal units, PLC software, Process control system}

Table 6. Attack severity for Goal 6

Attack	Severity for sub goal1		Severity for sub goal2		Severity for sub goal3	
	Level	Scale	Level	Scale	Level	Scale
MITM Attack	Low	5	Medium	7	Low	5
DOS	Low	5	High	9	Low	5
Sniffing	High	9	High	9	Medium	7
Privilege escalation	Medium	7	Medium	7	Medium	7
Unauthorized access	Medium	7	High	9	Medium	7
Flooding attack (PLC)	Low	5	Medium	7	High	9
Rootkit Attack	Low	5	Medium	7	High	9
Buffer overflow	Low	5	Medium	7	Low	5
Export hooking	High	9	High	9	High	9
Resource Exhaustion	Low	5	High	9	Low	5

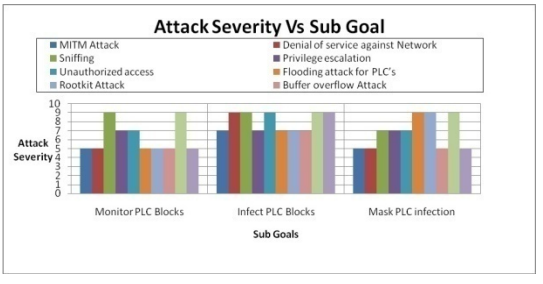

Fig. 10. Sub Goals and Attacks for achieving Goal 6

5 Conclusion

Stuxnet attack on SCADA system reemphasizes on extensive research in cyber security aspect of critical infrastructures. In this paper we have focused on one threat modeling technique to detect possible vulnerabilities attacks, and exploited resources in a system. An Attack Tree is a static threat modeling technique to capture the attacker's behavior as well as system behavior, this facilitates detailed analysis of an attack. We have designed novel Attack Trees for post Stuxnet attack scenario. For each Attack Tree, Goals and Sub goals are highlighted to clearly indicate the attacking approach. Common category of attacks has been discovered which were used for execution of Stuxnet attack. A one-to-many relationship between attacks and resources are discovered. A graphical representation of attack severity versus sub goals is helpful for quickly analyzing attacks in any component of SCADA system. This also shows how one attack opens the door for another attack and what resources were used for successful completion of attack. Using this information one can determine possible countermeasures depending upon cost and effort estimation.

References

1. Langner, R.: Stuxnet: Dissecting a Cyber warfare Weapon. IEEE Security & Privacy 9(3), 49–51 (2011)
2. http://www.wired.com/images../Symantec-Stuxnet-Update-Feb-2011.pdf
3. http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf
4. http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf
5. Stuxnet: The first weaponized software?, http://www.cs.columbia.edu/~smb/blog//2010-09-27.html
6. Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S.: Attacks against process control systems: risk assessment, detection and response. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011), pp. 355–366. ACM, New York (2011)
7. Schneier, B.: Attack Trees. Dr. Dobb's Journal 24(12), 21–29 (1999)
8. Khand, P.A.: System level security modeling using Attack Trees. In: 2nd International Conference on Computer, Control and Communication, IC4 2009, pp. 1–6 (February 2009)
9. Thesis, Efficient Semantics of Parallel and Serial Models of Attack Trees, http://www.cyber.ee/publikatsioonid/20-magistri-ja../JurgensonPhD.pdf
10. Supervisory Control and Data Acquisition (SCADA) Systems, http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf
11. Chen, T.M., Abu-Nimeh, S.: Lessons from Stuxnet. Computer 44(4), 91–93 (2011)
12. Paulson, L.D.: Worm Targets Industrial-Plant Operations. Computer 43(11), 15–18 (2010)
13. Ten, C.-W., Manimaran, G., Liu, C.-C.: Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans 40(4), 853–865 (2010)
14. Greengard, S.: The new face of war. Commun. ACM 53(12), 20–22 (2010)
15. Chen, T.M.: Stuxnet, the real start of cyber warfare? [Editor's Note]. IEEE Network 24(6), 2–3 (2010)
16. Stuxnet: rumors increase, infections spread. Network Security (10), 1–2 (October 2010)
17. Jeong, O.-R., Kim, C., Kim, W., So, J.: Botnets: threats and responses. International Journal of Web Information Systems 7(1), 6–17 (2011)
18. Morais, A., Martins, E., Cavalli, A., Jimenez, W.: Security Protocol Testing Using Attack Trees. In: International Conference on Computational Science and Engineering, CSE 2009, August 29-31, vol. 2, pp. 690–697 (2009)
19. Saini, V., Duan, Q., Paruchuri, V.: Threat modeling using Attack Trees. J. Comput. Sci. Coll. 23(4), 124–131 (2008)
20. Camtepe, S.A., Yener, B.: Modeling and detection of complex attacks. In: Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007, September 17-21, pp. 234–243 (2007), doi:10.1109/SECCOM.2007.4550338
21. Sungmo Jung,S. K., Song, J.-G.: Design on SCADA Test-bed and Security Device. International Journal of Multimedia and Ubiquitous Engineering 3(4) (October 2008)