Intrusion Perception Technology of the SCADA System of Oil and Gas Gathering and Transporting Based on FNN

Yang Fan[a], Xiedong Cao[b]
School of Electrical Engineering and Information, Southwest Petroleum University, Chengdu, China
[a]yfsy2010@163.com, [b]cowyco@126.com

***Abstract*—The security of the SCADA system has caused widespread concern in the world. This article first introduces the difference between SCADA system and traditional IT system, and the shortcomings of traditional intrusion perception technology. Then combine factors nerve theory, Establish the common factor neuron model of SCADA system and give it formal description. Research on the behavioral characteristics of malicious programs to extract major behavioral perception factors. Finally, use technology of API HOOK to achieve the perception of malicious behavior.**

Keywords-SCADA; Factors Neural Network; Perception; API HOOK

I. Introduction

SCADA system is widely used in power systems, water supply systems, petroleum, chemical and other fields of basic industries related to national lifeline, At the beginning of the development of SCADA system`s application, which is a relatively isolated physically isolated systems, and relatively safe, with computer technology and network communication technology applied in industrial control systems, information security has brought many problems. The “Earthquake Network (Stuxnet)” virus incident of Iranian nuclear power station has risen security of SCADA system, as the national basic industries key information system, to the height of the national strategic level.

Compared with traditional IT systems, the edge portion of the SCADA system of oil and gas gathering and transporting is not general computer traditionally. Structure of SCADA system enjoys vertical integration highly and has the characteristics of distribution and a master-slave relationship between the master node and the terminal node, rather than flat peering relationships of IT system. Besides, SCADA systems for production controlling has a high stable and real-time requirements, general safety products at risk, which is also differs from traditional IT systems. So security defenses means of Traditional information systems are not fully applicable to the SCADA system.

This study is a sub-topics of project of the National Natural Science Foundation “Research on FNN-based security defense modeling theory and simulation of SCADA network”. After analysis of the differences between SCADA system and the traditional IT systems, the factor neural network theory is applied to the security defense of SCADA system, factor neurons are used as the basic unit of execution of security and defense system, then explore a new way to achieve security and defense for SCADA systems by constructing analytic factor neuron model.

Intrusion perception is one of the effective means to guarantee system`s security. Traditional intrusion perception method includes two: misuse detection and anomaly detection [1]. Misuse Detection stores some modes or characteristics of known attacks in the repository in some form, if characteristics of audit data and mode of library rules match, then the intrusion occurred. Its biggest drawback is that it does not recognize new attacks, resulting in higher missing rate; Anomaly Detection, such as Intrusion Detection Expert System IDES, it first established normal behavior characteristic outline of system body, If the audit data in the system and the normal behavior characteristics have a large deviation, system is invaded. The ideal method of detecting abnormality can automatically distinguish between different behavioral according to the characteristics outline, but the reality is that in most environments the user's behavior is too random, If the intrusion detection is directly based on the simple rule matching, the large amount of false alarm and leakage phenomenon can be generated [2].

II. Factor Neural Network Theory

A. Factor and State Space

Factor is a category of cognitive and expression, which is in the process of cognitive things in abstract form, people use it to describe and cognize things, it is the basis for knowledge representation and reasoning, such as attributes considered when describing things and the various preconditions considered in the process of reasoning. Factor $f \in F$ can be regarded as a mapping，acting on a certain object $u \in U$，to obtain a certain state f (u). $f: D(f) \rightarrow X(f)$, wherein, $X(f) = \{f(u) \mid u \in U\}$ is state space of f [3].

B. Expression of Factor Neuron

Analytic factor neuron is a kind of factors neuron based on analytical model, through the use of function, rule and prototyping display of factor expression to complete expression and processing of knowledge and information. Analytic factor neuron is essentially a knowledge expression unit of knowledge description and the reasoning, It has not only descriptive factors which can be interpreted as fact and proposition, but also has reasoning function associated with the descriptive factors. A analytic factor neuron with reasoning functional can be expressed as:

$M = \{ < G, F, X >, < p, q, r >, < a, b > \}$

Among them, $< G, F, X >$ expresses structure, factors and state of analytic factor neuron;

p, q, r represents function of reasoning, distinction and internal control of executive neuron separately;

a is Input information; b is objective of unit reasoning.

III. TECHNICAL ROUTE AND DESIGN ANALYSIS

Combined with the key analysis of security and defense of SCADA system of oil and gas gathering and transporting, this paper mainly study and analyze from the perspective of secure and defense of system's host, where the starting point is precisely to determine behavioral characteristics of malicious programs. Because it can not only perceive the known attacks, but also has the advantages of perception of the unknown attack.

Malicious program behaviors are generated on the basis of malicious programs running action, In order to achieve the purpose of invading the system, it involves calling various application programming interface (API) functions provided by operating systems to complete intended function of code, such as file operations, registry operations, process/thread operations. It is through capturing sequences of these API function called by programs that we can visually see the program's behavior action, which is the perception of the invasion.

A. Definition of Program Behavior Factor

[Definition 1] The API function named as mark, complete an abstract description of the program behavior attributes, this description will be referred to the program behavior factors f.

[Definition 2] F is a collection of all the program behavior factor f, that is F={f}, called F is factor set of program behavior of all f.

B. Factor Expression of Knowledge

The knowledge of security and defense of the SCADA system is expressed by factor representation of knowledge. For the security defense of the host in SCADA system, the main factor is selected from three aspects of the file, registry, and process/thread operation.

In the domain U of SCADA system, O= {o} is the set of all the objects of cognitive and description in U. For the set o of each cognitive and descriptive object, A set of all the factors of o is expressed by a corresponding factor set F={f}.Each f in the factor set F exists a identified factor state space Xo(f) for the specific o.

[Definition 3] Atomic model of factor expression of knowledge: M(O)=<O, F, X>

Among them, O={FileOperations, RegOperations, Process/ThreadOperations}is set of object of cognition and description; F=(f) is a factor set of program behavior when describing O; X={Xo(f) |f∈F, o∈O} is factor space when F is used to describe O.

C. Expression of Knowledge of Neuron Model

To make neurons form an integrated analysis model that can centralize organizational structure, status information and rules of conduct of neurons together, enabling it to become a knowledge representation model and a knowledge application model. Choosing a reasonable knowledge storage mode is very important.

In terms of security research of SCADA system, the host contains many descriptive factors，such as host information and attack information . Its structure is strong, suitable to be expressed framework representation [4].

D. Architecture of Neuron

From the viewpoint of automatic machines, an analytical factor neuron likes a mini-automatic machine, which has a set of states with factor expression and a set of state transition rules, when the external input triggers the automatic machine, automatic machine executes the corresponding operation according to the perception information and carries on the status conversion, and the output unit responds finally according to the output response function.

From this point of view, the internal architecture of analytical factor neuron of SCADA can be designed into five parts: perception module, discrimination module, reasoning module, factors of knowledge library, output modules [5]. As shown in Fig.1.

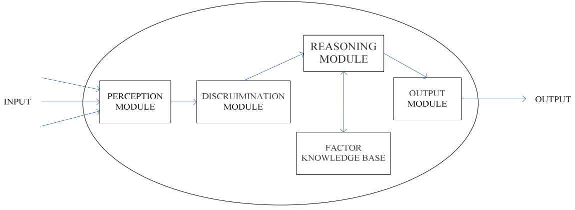

Figure 1. The internal architecture of analytical factor neuron

The perception module this paper studies mainly is responsible for the interaction between the analytical neuron and the outside world, and is the channel of the neuron's perception of the outside information, which includes information perceptron of environmental change and information receiver for communicating with other neurons, and enjoys the functions of perceptions of outside information, data pretreatment, receive information transmitted from other analytical factors neurons transmit and so on.

IV. FUNCTION REALIZATION

A. Extraction of Program Behavior Factor

To complete the intrusion perception, we first need to understand exactly which program behaviors need to be extracted to build behavioral factors. Through analysis of the large number of samples from registry operations, file operations and process/thread operations. Sensitive behaviors are extracted as behavioral factors. As shown in Table I

TABLE I. BEHVIORAL FACTORS TABLE

operation	action	behavioral factors
	Create files	CreateFileA OpenFile
	Write files	WriteFile ,WriteFileEx
	Copy files	CopyFileA, CopyFileExA

operation	Move files	MoveFileA, MoveFileExA
	Replace files	ReplaceFileA, RepalceFile
	Delete files	DeleteFileA
	Find files	FindClose, FindFirstFileA FindNextFileA,FindResourceA
	Search Directory	GetSystemDirectoryA, GetWindowsDirectoryA CreatDirectoryA
	Remove directory	RemoveDirectoryA
	Set attributes	SetFileAttributesA, SetFileTime
registry operation	create	RegCreateKeyA
	delete	RegDeleteKey
registry operation	modify	RegSetValueEx
	Read query	RegQueryValueExA RegOpenKeyEx RegCloseKey RegEnumKeyExA
process/ thread operation	create	CreateThread,CreateProcessA
	terminate	TerminateProcess
	Remote thread	CreateRemoteThread
	Search Thread	EnumProcesses GetModuleBaseNameA

B. Design of Perception Module

Operations of application under Windows are completed by API functions, so in order to perceive the behavior of a program, the call operations of these API functions are needed to be intercepted to further analyze their behavioral factors, judge and decide whether to interfere with its implementation process, so as to achieve monitoring and control of malicious programs.

Principle of API HOOK technology is hook processing of API functions, when the program calls API function, hook calls first and then jump to perform prepared hook function, rather than to perform the actual API function, thus call of API functions can be intercepted. According to interception of different levels, API HOOK can be divided into user-level hooks and kernel-level hooks. User-level hooks include mainly modifying the output address table and Inline HOOK. kernel-level hooks include mainly soft interrupt of interception of system service (INT 2EH)、system service descriptor Table (SSDT HOOK)、modify the kernel objects and filter driver of file system[7].

This paper mainly uses combination of methods of SSDT HOOK and filter driver of file system, which are both working at the kernel level, and need to write the driver. The realization of a function at the user level may sometimes correspond to multiple API, but the final call in kernel-level is the same kernel-level API, so the interception at kernel-level is less likely to be bypassed. Therefore, this article uses SSDT HOOK technology to perceive operations of registry and process/thread, and uses file filter driver to perceive file operations.

1) Perception of operations of registry and process/thread

SSDT (System Service Descriptor Table) essentially is series function entry address table of NtXXX function stored in the kernel. When the system kernel is loaded to run, the entry address table which storages system service functions (NtXXX) will be created. In order to facilitate the achievement of quickly accessing service functions in the table by index number, SSDT storages entry address of system service function by order table, so long as we know the first address of the table and a NtXXX function index in the table, it can be very facilitate the realization of calls.

2) Perception of file operations

In view of the file system, user processes on the disk files operations, including create, open, read, write and other operations, first to call the relevant API function, and then call the corresponding service by the WIN32 subsystem to represent the process to send requested operation. I / O manager receives from the user-level I / O requests, then construct I / O request packet (IRP) and sent to the file system driver, thereby achieving a request for a specific file operations.

In this paper, the file system filter driver is designed between the I / O manager and file system driver, because before the IRP is sent to the target device object, I / O Manager will first determine whether target device mount additional device object, if there is, then it will be first sent IRP to the additional device, then processed by driver which belongs to additional device, and finally sent to the target device to complete the requested operation. Therefore, file operations request can be intercepted before it reaches to the target device and dealt with it accordingly.

V. EXPERIMENTAL RESULTS AND ANALYSIS

In this study, the data set is KDD Cup 1999 data set[9], the data set is widely used in the invasion perception test, which is one of the standard test sets for invasion perception system. Before the experiment data sets need to be coded into the numerical type which can be recognized by neural network, and finally standardize and normalize. Add five types of marked data sets: Normal: normal data; DOS: Denial of Service; R2L: distal unauthorized access; U2R: unauthorized access of super user; PROBE: system vulnerability detection and balance [8].

Composition of experimental data sets is represented by Table II.

TABLE II. COMPOSITION OF EXPERIMENTAL DATA SETS

	Normal	DOS	Probe	U2R	R2L	new
test1	3300	200	200	100	50	30
test2	3500	180	180	90	40	40

Among them, new is test of new attack.

The model is verified by five types of marked data sets and experimental results is represented by Table III.

TABLE III. EXPERIMENTAL RESULTS

test	NOR	DOS	Probe	U2R	R2L	new	FP	NF
1	3201	180	182	88	39	19	0.027	0.12
2	3390	160	167	73	31	28	0.032	0.013

FP, namely False Positive, is the probability of intrusion perceived when there is no intrusion.

NF, namely False Negative, is the probability of intrusion non-perceived when intrusion occurs.

Experimental results show that the application of neural networks to intrusion perception, which enjoys the higher accuracy rate, the lower false positive rate and negative rate and the higher perception efficiency.

VI. CONCLUSION

According to the characteristics of the SCADA system of oil and gas gathering and transporting and the shortcomings of traditional Intrusion of perception, the analytic factor neuron model of security and defense of SCADA is built by combination with factor neural networks, which has a high accuracy perception rate and can perceive unknown attacks. A new method and technology is provided for the research on security and defense of SCADA system.

REFERENCES

[1] MARTIN B, ROSSOUW S, Utilising fuzzy logic and trend analysis for effective intrusion detection [J]. Computers and Security, 2003, 22(5):423 - 434.

[2] IIGUNK, KEMMERER A. State Transition Analysis: A Rule-based Intrusion Detection App roach [J]. IEEE Transaction on Software Engineering, 1995, 21(3):181 - 199.

[3] Z. L. Liu, Factor neural network theory and application. Guiyang: Guizhou Science and Technology Press, 1994.

[4] H. S. Wei, Neural Network Structure Design Theory. Beijing: National Defense Industry Press, 2005:33-39.

[5] C. X. Guo, Z. L. Liu, Y. Tao, Research on attack and defense analysis model of virtual network ［J］.Computer Engineering and Applications，2008，44(25) :100-103

[6] C. X. Guo, Z. L. Liu, Z. N. Zhang, Knowledge factor space model of network attack [J]. Telecommunication technology, 2009, 49(10) :11-14.

[7] B. X. Ni, Windows hook technology and Realization [J]. Computer and modernization.2007(01)

[8] X. R. Liu, Review of Network attack classification technology ［J］. Journal of communication. 2004，25(7) : 30-36.

[9] Z. W. Liu, Y. Cai, B. Chen, KDD Application of KDD in Intrusion Detection J]. Microcomputer and Application, 2003, 12:55-58