MATEC Web of Conferences **44**, 02032 (2016)
DOI: 10.1051/matecconf/20164402032
© Owned by the authors, published by EDP Sciences, 2016

The Implementation of a Vulnerability Topology Analysis Method for ICS

Yi Lin Yang[1,2],Ji Teng Wang[1,2], Guo Ai Xu[1,2]

[1]*Beijing University of Posts and Telecommunications, Beijing, China*
[2]*NEL of Security Technology for Mobile Internet, Beijing, China*

Abstract. Nowadays Industrial Control System (ICS) is becoming more and more important in significant fields. However, the using of the general facilities in these systems makes lots of security issues exposed. Because there are a number of differences between the original IT systems and ICSs. At the same time, the traditional vulnerability scan technology lacks the ability to recognize the interactions between vulnerabilities in the network. ICSs are always in a high risk state. So, this paper focuses on the vertex polymerization of the topological vulnerability analysis. We realized a topological analysis method oriented ICSs on the basis of achievements at home and abroad. The result shows that this method can solve the problem of the complex fragility correlation among industrial control networks.

1 Review

Currently, ICSs have a wide range of applications in Chinese electric power, water conservation, sewage treatment, oil and gas, chemical, transportation, pharmaceutical and other industries. ICS has been an vital component of the national security strategy[1].

However, with the deep integration of informatization and industrialization, ICSs are increasingly using common protocol, common hardware and common software, and using a variety of ways to connect the Internet and other public network.This causes that viruses, Trojans and other threats are diffusing in the ICSs. ICSs' security issues have become increasingly prominent [2]. At the same time, since there are many differences between traditional enterprise IT systems and ICSs, the security measures of IT systems are often not well suited to ICSs. This often leads to accidents due to system failure. Many critical control systems are at high risk condition.

This paper will be based on the topological analysis techniques to study the vulnerability topological analysis techniques oriented ICSs. Compared to some related research progress, this paper makes improvement on the number of vertexes, which need to be analyzed by target topology. The advantage is reducing the cost of network administrators' exploring the industrial system vulnerabilities, as well as the time, labor and other costs.

2 Topological analysis technology oriented to ICS

Based on the existing research[3], this chapter will explain the topology analysis technology of the ICS. When analyzing the security of the ICS, the analysis flows of the topology hidden trouble analysis technology in this paper can be summarized as:

1 to read the ICS network asset allocation file provided by the user;

2 to implement the prototype system, and output the original topology vertex's and arc's information;

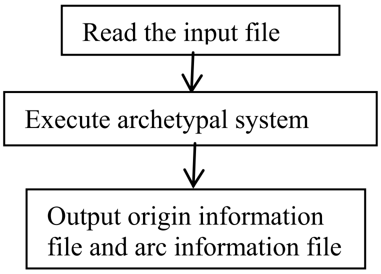
3 to analyze the target topology structure structured by the vertex information and the structure of the arc information in the second analysis;

4 to run vertex aggregation algorithm to execute the initial optimization and depth optimization of the target topology;

5 to get the output information of the algorithm in the fourth analysis and provide the main interface module of the tool;

6 to make topological analysis and show the results of hidden trouble analysis[4].

The overall work flow of this method is shown in Figure 1.


Read the input file
Execute archetypal system
Output origin information file and arc information file

Article available at http://www.matec-conferences.org or http://dx.doi.org/10.1051/matecconf/20164402032

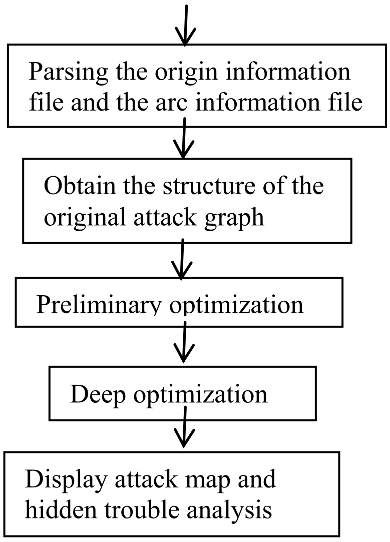

Parsing the origin information file and the arc information file
Obtain the structure of the original attack graph
Preliminary optimization
Deep optimization
Display attack map and hidden trouble analysis

Figure 1. system's work-flow

2.1 vertex aggregation algorithm

In this paper, a simple node aggregation algorithm is designed. Through this algorithm, on the base of retaining all the vertexes' information of the prototype tool's target topology[5], we simplified all the vertexes of the original topology twice, and eventually generated a topology analysis result that the vertex number was reduced to the same number of the device in the described network. And the vertex information belonged to the same device in the original figure will be collected to corresponding device vertex in the new figure. The network device we said includes the device used by attackers. This algorithm is described as follows:

Input: The information of the target topology described by the prototype tool includes the vertex information and the arc information.

Output: An analytic topology, in which the number of vertexes is equal to the number of devices in the described network, the vertex information is not reduced. And the described attack path is consistent with the input graph.

First, we will analyze the original topology of the prototype tool. Three kinds of vertexes of the original topology are the attack steps vertex of oval, the right vertex of the diamond, which means it can obtain the right from its predecessor node, and the configuration information vertex of the rectangle. In these three kinds of vertexes, the key point is the right vertexes, because they describe the process that the attacker obtains the right to keep close to the target he wants to achieve, and they are most able to explain the attacker's attack path. The secondary vertex is the vertex of the attack's starting position described by the configuration information vertex, because it describes the origin of the attack path. We first define three classes of vertexes before the introduction of vertex aggregation algorithms.

Definition 1 (right vertex P-Node): A P-Node represents a certain level of authority derived from the derivation of the pioneer vertex.

Formal definition is:

$$\forall n2 \in P-Nodes, \exists n1 \in P-Nodes \bigcup C-Nodes$$

is n2's ancestor vertex,

there exists a reachable simple oriented path from n1 to n2.

Definition 2 (configuration information vertex C-Node): C-Node represents a network configuration.

Formal definition is:

$\forall cn \in C-Nodes$,

cn is the element of Configuration-condition.

The Configuration-condition represents a collection of network configurations.

Definition 3 (attack step vertex S-Node):

A S-Node vertex refers to a single attack will be triggered when all its preconditions(S-Node or P-Node)are satisfied.

Formal definition is:

if ({pn1, pn2,…,pni} ∈ P-Nodes
  or {cn1, cn2,…,cnj} ∈ C-Nodes
  and {pn1, pn2,…, pni , cn1, cn2,… , cnj} ∈ Rules)
  then {pn1, pn2, , pni , cn1, cn2, , cni}
sni ∈ S-Nodes

The Rules represents a collection of attack rules.

In the three kinds of vertexes, S-Node is the vertex of the logical AND type; C-Node and P-Node are the vertexes of the logical OR type[6] .

2.2 Algorithm design

Preliminary optimization

In contrast, other configuration information vertexes can be used as a supplementary information of access information, to describe the necessary conditions of obtaining a certain permission. While all the configuration information vertexes' in-degree in the original figure is 0, and their out-degree is 1. Therefore, after reserving the configuration information to permission information's subsidiary information, all the other configuration information vertexes, together with the related edges, can be removed from the original figure.

At the same time, the attack steps vertex describes the method to obtain the other permissions when the configuration information and some rights are met. So, in the original topology, the attack step vertex is the ancestor of the right information vertex. Thus, the information of the utilization method described by the attack steps vertex can be aggregated to the right vertex of their children' position. At the same time, the arc which points to it will point to the right vertex of its descendants. Then we can remove the attack steps vertex from the original figure.

After the above operation, the first step of original topological vertex aggregation algorithm is completed. Now the figure only retains the permissions vertex, the attacker's first position vertex, all arcs connected to these vertexes, and all information keeping the other vertexes in the original figure. If you do not have all information of the other vertexes to display, you can display when the users need to obtain information. After the initial optimization of the vertex aggregation algorithm, the intermediate rendering effect of the analytic topology is shown in Figure 2.

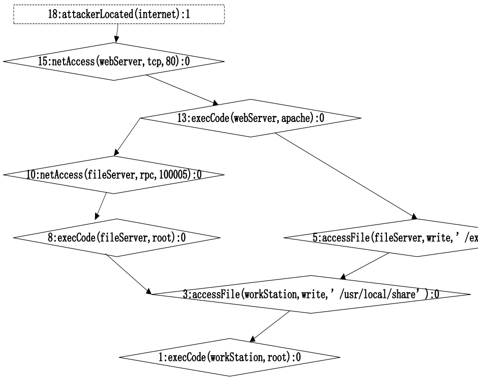

18:attackerLocated(internet):1
15:netAccess(webServer, tcp, 80):0
13:execCode(webServer, apache):0
10:netAccess(fileServer, rpc, 100005):0
8:execCode(fileServer, root):0
5:accessFile(fileServer, write, ' /export'):0
3:accessFile(workStation, write, ' /usr/local/share'):0
1:execCode(workStation, root):0

Figure 2. The intermediate rendering effect of the analytic topology after the initial optimization.

Deep optimization

After the initial optimization, the decrease of the topological vertexes' number has been extraordinarily sizable. In this case, the vertex number of the prototype tool's analytic topology, which contains 26 vertexes, has been reduced to 8, and the number of nodes has been reduced to 70%. But it has not reached the goal of the algorithm, that is, the number of vertexes is equal to the number of targets device described by the network. The reason why the number of vertexes after the initial optimization is greater than the number of devices described by the network is that multiple access behaviours occur on the same device sometimes.

In order to achieve this goal, we have to aggregate multiple permissions' acquisition behaviour that occurs on a device to the same vertex. And we describe these permissions in the order of obtaining permission in this vertex.

After the deep optimization above, the output analytic topology can be used as the final output of the algorithm. The rendering effect of the analytic topology after the deep optimization of the vertex aggregation algorithm is shown in Figure 3.

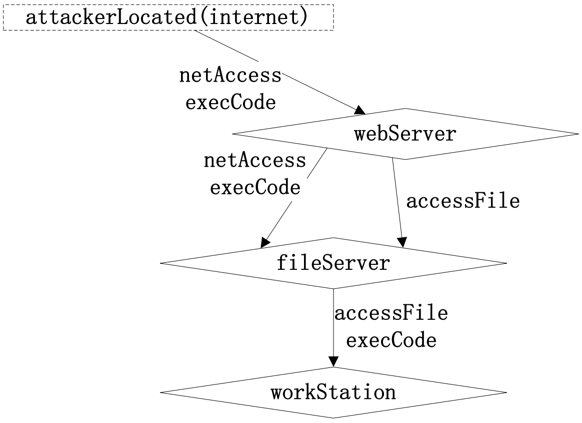


Figure 3. The rendering effect of the analytic topology after the deep optimization of this algorithm.

After gathering the multiple access happened on the same device to the same point, the attacker's attack process can be showed on the network topology of the actual ICS, and it's marked in red in the realization of the technology. This can help to identify the vulnerable hosts in the target network.

3 Technical realization and experimental analysis

After the two-step optimization of the algorithm described in the last chapter, in order to make the display effect more vivid and intuitive, we need to beautify the vertex shape of the graph in the realization of the topological analysis technology. We can use sketch map representing the corresponding equipment to describe the vertex. This has been overstepped the required work scope of the algorithm, and these work is mainly done in the technology realization boundary.

In real applications, the reduction of the vertex's scale in the analytic topology brings a shorter emergency response time for the administrator, and thus be more agile to deal with the fragile problem of the industrial control network. However, this subjective situation cannot be verified in this paper.

In order to verify the advantages of the technology described in this paper, a new approach is adopted. The implementation of the algorithm is implemented in the target network of 3, 10, 20 and 50 scales. The difference on the vertex number between the two kinds of optimization and the existing technology is compared in this paper.

Experiment 1:

The analytic topology before Ou technology's optimization is compared with the analytic topology obtained in this paper on the vertex's number. Experimental results are shown in the following diagram.

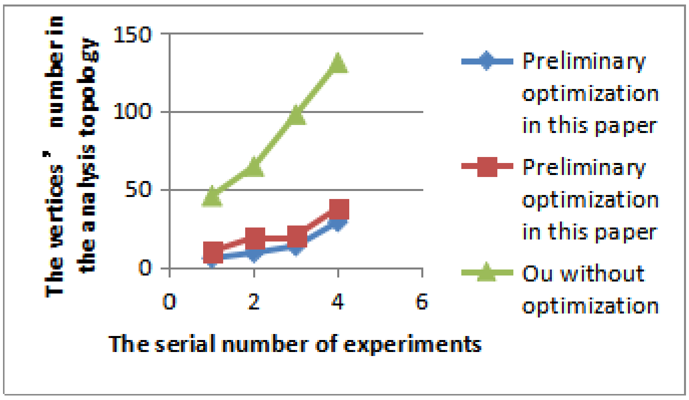


Figure 4. Experiment 1: the vertexes number's comparison in the existing technology without optimization.

What is shown in Figure 4 is that, after preliminary optimization, the vertexes scale in the topology has been significantly reduced to about 10%~30% of the existing technology. Then, after the deep optimization, the number of vertexes has been reduced in a small extent. The experimental data shows that, compared with other technologies, the number of vertexes in this paper is drastically reduced, which will lead to a lot of liberation for the vulnerable point location of topological analysis.

Experiment 2:

The vertexes number of the analytic topology with the optimization of the Ou technology is compared with the analytic topology obtained in this paper's algorithm. Experimental results are shown in the following diagram.

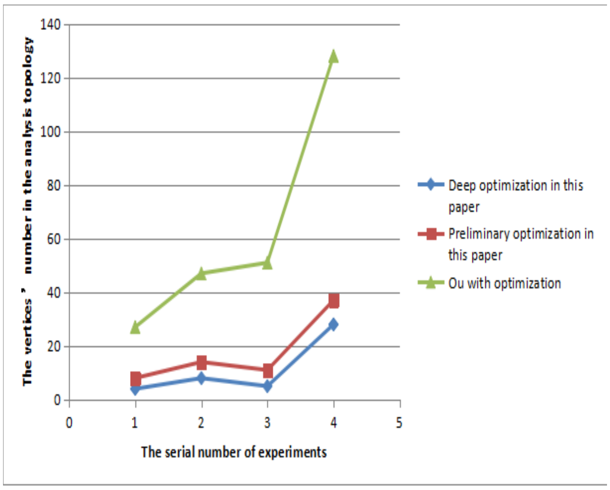


Figure 5. Experiment 2: comparison of the number of vertexes in the existing technology optimization

Ou technology itself also has the ability to optimize, we compare the analytic topology after this optimization with the technology of this paper again. After comparing Figure 4 with Figure 5, we can find that Ou technology's own optimization ability is not stable. Sometimes we can get very good optimization, sometimes cannot. But this paper can make notable optimization on the same analytic topology. This experiment shows that the optimization results of the proposed algorithm in this paper is more stable than Ou's existing technology.

4 Summary

In the field of ICS, this paper designed and implemented an ICS topology analysis technology based on graph data structure. This technology can be used in small and medium-sized industrial control network to analysis at the security hidden trouble. It also describes the attackers' might-taken attack path in compromising the network process, and highlight the fatal weakness in the network. So it can play an assistant function about forecast in the security defence of the ICS.

This technology can be used in the ICS's network security analysis. Compared to the previous research, this paper has a breakthrough in the application domain. At the same time, compared to the previous analysis, the results of this paper are more obscure and complex. After two-step optimization, the technology cooperates with the graphical interface design to show a simple, clear and intuitive topological analysis results. To some extent, the burden of network administrators on the identification of network fragility can be reduced. And the network administrator users' experience faced to ICS become friendlier.

Acknowledgment

This work is supported by National Natural Science Foundation of China Project (61302087, 61401038, U153 610079).

References

1. Peng Cheng. Information Security of Industrial Control System – China Information Security, 2014(1):31—32.
2. Qinzhi Wei. Industrial Network Control System Security and Management-Measurement& Control Technology,2013(2).
3. Shuai Zhang. Security situation and risk analysis in industrial control systems – In aspect of the risk analysis in security of ICS, 2012, 4: 46—48.
4. Ye Zhang. New focus on information security – Security of industrial control system, 2012, 4: 46—48.
5. Xinming Ou. A Logic-programming Approach to Network Security Analysis. PhD thesis, Princeton University, 2005.
6. Congli Ling. Analysis and Modeling of Vulnerability in Industrial Control System. PhD thesis, Zhejiang University, 2013.