The Research on Attack Threat Sensing based on "Software Security Sensor"

Yuan Zhao1,2, Qiangbo Liu1, Dingyi Fang1,2, Huaijun Wang1,2, Cong Zhang1,2
1 School of Information Science and Technology, Northwest University, Xi’an, China
2 NWU-Irdeto Network-information Security Joint lab (NISL)
Corresponding Author: zhaoyuan19890807@126.com

Abstract—Aim at the different attack threats the running software faced with during reversing, a method of sensing attack threats based on "software security sensor " is proposed in this paper. And the instance has demonstrated that the method is effective and feasible. Drawing lessons from the thought of physical sensors, the code snippet which is used to sense the attack threats is called "software security sensor", SwSensor for short. Firstly, the attack threats and their features are analyzed; then the design of the corresponding SwSensors and the delimiting of sensed areas is discussed in detail; finally, the layout model based on the multi-level gateway in physical sensor network is described.

Keywords—Attack threat; Sensing; Software Security Sensor; Code Blocks Dependency

I. INTRODUCTION

The software runs in white box attack environment[1], leading to the key information exposed to attackers further. Meanwhile, the continuous development of attack tools and methods makes the white box attack environment more dynamic, complex and unpredictable[2].

Traditional software protection methods, such as, encryption, obfuscation belong to the static protection because the protected software cannot adjust their execution paths dynamically.2011, Collberg put forward the idea of dynamic protection, who thought that the factors including speed, agility, unpredictability, vigilant monitoring, defense in depth, and renewability of defenses are all necessary to ensure long-lasting defenses[3]. So, to make the protected software updated the defense with the changes of environment and dynamically game in the terminal with the attacker is a new idea to explore dynamic protection further. The first problem is how to make the running software sensed the attack threats in white box attack environment.

Reversing attack will cause the changes of elements in white box attack environment, which is the fundamental basis to sense attack threats. Usually, the reverse analysis process can be divided into three stages: the disassembly, dynamic and static analysis and decompiling[4], as shown in figure 1. The first stage is to disassemble the binary code into assembly code. The second is to understand the functions and semantics to get control flow, data flow and algorithm etc. The last is to decompile assembly code into source code. However, the differences among high-level languages result that the attack effect based on decompiling is not ideal. Attackers attack the first two stages usually by means of some mature tools, such as OllyDbg, IDA, to set breakpoints, memory dump, etc. Among them, the dynamic and static analysis is the process of human thinking, and does not change the elements of environment. Therefore, the attack threats that the running software is faced with in white attack environment can be divided into three types: debugging attack, dumping attack and tampering attack from the perspective of reverse analysis.

Figure 1. Reverse Engineering and Attack Threats.

II. RELATED WORK

There are some related research results at home and abroad.

- Anti-debugging techniques based on detecting the changes of environment elements.
- Tamper-proof techniques based on multi-point guards.
- Sensing techniques with intelligent decision.

Arash Salehpour et al[10] developed an intelligent guard which could monitor the changes of environment and make decisions on whether continuing to execute in the software life cycle. Artificial intelligence is introduced in this technique to make the terminal software be self-adjusting with the changes in the environment. Due to the intelligent...
guard and protected software are separated, attacking on intelligent guard itself becomes a bottleneck.

III. ATTACK THREATS SENSING BASED ON SWSENSOR

A. Overview

![Mechanism of Sensing the Attack Threats](image)

Figure 2. Mechanism of Sensing the Attack Threats.

We will introduce the basic concepts firstly.

B. Basic Concepts

- **Sensed elements**
  Refer to the factors which will cause the changes of white box environment or affect the running software, such as, the debugger will modify the flag bit of Beingdebug. And the other factors, such as, the sequence of API, which can reflect the changes of software itself, also belong to sensed elements.

- **Set of attack threats features**
  Attack threats can be divided into debugging, dumping and tampering. Different attack threats will change different sensed elements and the subset of which can identify different attack threats are called set of attack threats features.

- **Security dependencies among code blocks**
  Refer to the software attributes used to identify the influence on other code blocks when a code block is being attacked, such as, invoking, data dependencies, etc.

- **SwSensor**
  Assembly code used to sense the attack threat in running time, such as, the snippet code of integrity checking.

C. Method of Sensing Attack Threats

**Step1.** Collect the sensed elements of debugging, dumping and tampering based on attacking experience and knowledge. Marked as \( f_g = \{\text{name}, \text{way}, \text{value}\} \), \( f_g \) represents a sensed element, \( \text{way} \) represents the usage of \( f_g \), \( \text{value} \) means the secure value of \( f_g \).

Construct the attack threat feature library as following. \( DgThreat \) refers to the debugging attack threat, \( DpThreat \) refers to the dumping and \( TpThreat \) refers to tampering attack threat.

\[
AtfLib = \begin{cases} 
 DgThreat : f_{11}, f_{12}, \ldots, f_{1n} \\
 DpThreat : f_{21}, f_{22}, \ldots, f_{2n} \\
 TpThreat : f_{31}, f_{32}, \ldots, f_{3n} 
\end{cases}
\]

**Step2.** Construct the corresponding software security sensors library, marked as \( SwSensorLib \), according to \( AtfLib \). The design principle is that judge whether the software is in a secure state or not by identifying the features of attack threats is normal or not. The details are shown here:

- Design the functional template of SwSensor, marked as \( SwSensorTemplate = \{At_i, ftset, Parameter,\} \), \( At \) represents the type of attack threat, \( ftset \) represents the subset of features, \( Parameter \) presents the parameter list, such as, the start address of sensed area.

- "Feature value" is used to reflect different attack threats, \( Feval \) for short. The sensing algorithm is designed of randomly selecting several features and normalizing them to get \( Feval \), marked as \( Algorithm \).

- Use the deformation engine to diversify the different \( SwSensorTemplate \) to construct the \( SwSensorLib \).

\( SwSensorLib = \{SwSensorTemple, Swsensorset,\} \), \( Swsensorset \) represents the set of Swsensors coming from \( SwSensorTemple \).

**Step3.** According to the security dependencies and division rule among code blocks, delimit the sensed areas.

- According to the attack experience and knowledge, obtain the security attributes \( CSAttr \) and form the security dependencies among code blocks.

\( CodeSecDep = \{CSAttr1, CSAttr2, \ldots, CSAttrn\} \).

- Delimit the sensed areas of the being protected software \( SArea = \{CodeSecAttr, parameter\} \) then form \( SwSensorArea = \{SwArea1, SwArea2, \ldots, SwArea_{n}\} \).

**Step4.** Generate the layout scheme based on multi-stage gateways model.

- Matching suitable SwSensor for the different sensed area and setting their parameters. Marked as \( \forall SwSensor_i^k \in SwSensorLib, Swsensor_i^k \mapsto SArea \).

- Setting the parameters of SwSensors based on minimum coverage theory of graph. Regard the chosen SwSensors as the vertices of graph, the sensed scope as edge sets, construct associated matrix and adjust the sensed scope repeatedly to get the minimum coverage vertex set. And considering the security dependencies among code blocks, level classification is carried out on the chosen SwSensor and the multi-level gateway structure in accordance with self-security is constructed.

**Step5.** Reconstruct the protected software to make the SwSensors triggered in the appropriate time.

IV. INSTANCE AND EVALUATION

A. Attack Threats Lib

Extract several features of three attack threats below.

- \( DgThreat \) features: the execution time, the breakpoint;
- \( DpThreat \) features: the API sequence;
- \( TpThreat \) features: code checksum and control flow.

The description of attack threat library is shown in table 1.
TABLE I. DESCRIPTION OF ATTACK THREAT LIB

<table>
<thead>
<tr>
<th>Attack Threat</th>
<th>Sensed elements</th>
<th>Name</th>
<th>Way</th>
<th>Sec_val</th>
</tr>
</thead>
<tbody>
<tr>
<td>DgThreat</td>
<td>f1</td>
<td>ExeTimevar</td>
<td>When the process is being debugged, the debugger event handling code, step instructions etc will occupy CPU cycle. If it takes between adjacent orders far more than conventional, means the process is being debugged.</td>
<td>[t1,t2]</td>
</tr>
<tr>
<td></td>
<td>f12</td>
<td>Breakpoints</td>
<td>Int3 breakpoint will modify a byte memory into 0xCC.</td>
<td>Not 0xCC</td>
</tr>
<tr>
<td>DpThreat</td>
<td>f21</td>
<td>APISeq</td>
<td>When fixing ImageSize, call for API sequence below: GetProcessBaseSize, GetProcessPath, CreateFile, ReadFile</td>
<td>Not this API sequence</td>
</tr>
<tr>
<td>TpThreat</td>
<td>f31</td>
<td>Checksum</td>
<td>Checksum is always same without tampering attack.</td>
<td>SUM</td>
</tr>
<tr>
<td></td>
<td>f32</td>
<td>ControlFlow</td>
<td>Code the control flow and test if it is changed in runtime.</td>
<td>[a1,a2,…an]</td>
</tr>
</tbody>
</table>

TABLE II. DESCRIPTION OF SWSENSOR TEMPLATE LIB

<table>
<thead>
<tr>
<th>Template</th>
<th>Attack Threat</th>
<th>Features</th>
<th>Parameter list</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST11</td>
<td>DgThreat</td>
<td>f1,f12</td>
<td>&lt;startaddr,endaddr,val&gt;</td>
</tr>
<tr>
<td>ST12</td>
<td>DgThreat</td>
<td>f11</td>
<td>&lt;startaddr,endaddr,[t1,t2]&gt;</td>
</tr>
<tr>
<td>ST13</td>
<td>DgThreat</td>
<td>f12</td>
<td>&lt;startaddr,endaddr,0xCC&gt;</td>
</tr>
<tr>
<td>ST21</td>
<td>DpThreat</td>
<td>f21</td>
<td>&lt;startaddr,endaddr,APIseq&gt;</td>
</tr>
<tr>
<td>ST31</td>
<td>TpThreat</td>
<td>f31</td>
<td>&lt;startaddr,endaddr,SUM&gt;</td>
</tr>
<tr>
<td>ST32</td>
<td>TpThreat</td>
<td>f32</td>
<td>&lt;startaddr,endadr, {a1,a2,…an}&gt;</td>
</tr>
</tbody>
</table>

For example, the two sensed elements of DgThreat from table 1 are combined to produce three subsets of features: \{f11, f12\}, \{f11\} and \{f12\}. Then, compute the “feval” of each subset only includes \{f11\}, so its “feval” can be directly identified as \([t1, t2]\), but the first subset includes \{f11, f12\} which do not belong to the same dimension and must be computed by normalizing.

2) Sensing algorithm

Sensing algorithm
- Read fij from AtLib
- Normalize(fij) to get VAL
- Compare VAL, parameters.val
- If unequal Broadcast()
- else Continue

The Normalize (fij) is defined by user. Broadcast () transfers the attack information.
We define the Normalize (fij) below:
1. ST11: t2-t1+0xcc;
2. ST12 : (t2-t1)* t1;
3. ST13: 0xcc;
4. ST21: 1111;
5. ST31: SUM+a1+a2+...+an;
6. ST32: SUM;
7. ST33: a1+a2+...+an.
A part of pseudo codes of templates are shown in table 3.

TABLE III. PSEUDO CODE OF SWSENSOR TEMPLATES

<table>
<thead>
<tr>
<th>Template</th>
<th>ST11</th>
<th>ST12</th>
<th>ST32</th>
</tr>
</thead>
<tbody>
<tr>
<td>move eax, t2</td>
<td>Invoke GetTickCount move ebx, eax</td>
<td>add edx, checksum</td>
<td></td>
</tr>
<tr>
<td>move ebx, eax</td>
<td>Invoke GetTickCount move ebx, eax</td>
<td>mov eax, startaddr for:</td>
<td></td>
</tr>
<tr>
<td>sub eax, ebx</td>
<td>cmp eax, endaddr jg end</td>
<td></td>
<td></td>
</tr>
<tr>
<td>add edx, 0xcc</td>
<td>mov ebx, dword[eax] add ebx, edx</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sub eax, feval</td>
<td>move ebx, dword[eax]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jz label</td>
<td>add edx, 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>continued label:</td>
<td>cmp eax, endaddr jg end</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcast</td>
<td>mov ebx, dword[eax]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>label: Broadcast</td>
<td>cmp eax, endaddr jg end</td>
<td></td>
<td></td>
</tr>
<tr>
<td>end:</td>
<td>mov ebx, dword[eax]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

B. SwSensor Template Lib

1) Design of SwSensor Template
Combine the different sensed elements of one attack threat to generate the multi-subsets of features.

C. Delimiting the Sense Area

1) Security dependencies
We adopt the control dependency\(^{[12]}\) as the security dependency. There are three atomic control dependencies based on the functions granularity\(^{[13]}\), as figure 4 shows.

The weighted directed graph commonly is used to indicate the control dependencies among code blocks, as shown in figure 5. Among, \(P \rightarrow Q\) represents \(P\) depends on \(Q\), the weight means the degree of control dependency.

Figure 3. Deformation engine.

Figure 4. Three atomic control dependencies.

Figure 5. The control dependency among code blocks.
Step1: Draw the control dependency graph without weight;
Step2: List the paths starting from the node with zero indegree and ending in that of zero out-degree;
Step3: The weight of one edge equals to the outdegree of the head node plus the weight when it is tail node. That is, the weight of “Q→W” in “P→Q→W” equals to the outdegree of Q plus the weight when Q is tail node. For the ring node as the tail node, the weight of the edge plus 1.
Step4: Repeat step 3.
So, we analyze the weight of each edge in figure 5 here:
1) ABCG, 2) ABDE, 3) ABDG, 4) ABDHH, 5) AE, 6) FDE, 7) FDG, 8) FDHH.
And then, mark the weight from the node with zero indegree: 1) A2B4C5, 2) A2B4D8E, 3) A2B4D8G, 4) A2B4D8H9H, 5) A2E, 6) F1D8E, 7) F1D8G, 8) F1D8H9H.

2) Assembly of Sensors Areas
Sort the code blocks according to control dependency with key code block from strong to weak, and then select first n related code block as the assembly of Sensors areas.
As shown in figure 5, it is assumed that “D” is the key block, sort the other code blocks according to the control dependencies with “D” from strong to weak: DEGHBF. In this case, select “DEGHBF” as the assembly of sensors areas.

D. Layout schema and Reconstuction
1) Matching SwSensors with code blocks
Choosing the appropriate SwSensor for different sensed area according to two principles: ① Select SwSensor according to the code block's own features; ② Considering the performance cost, select the smallest SwSensor only if meeting the first principle.

2) Layout model based on multi-layer gateway
It is to assign a value to the parameters. Like the left in figure 6. The control dependencies among the block codes aren’t changed in fact and just increased several layers of SwSensor. The sensed attack information is passed to the higher layer, which is similar to physical multistage gateway.

Figure 6. Layout model based on multi-layer gateway.

3) Reconstuction
The chosen SwSensors are embedded into the code blocks in the assembly instruction level to generate the protected software. Like the right in figure 6.