Firmalice

Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware

Yan Shoshitaishvili

Ruoyu "Fish" Wang

Christophe Hauser

Christopher Kruegel

Giovanni Vigna

UC Santa Barbara
The Rise of Firmware
WELL, BASICALLY I VOMITED ON A CANVAS AND THEN LET IT DRY.
Emergence of Backdoors

Heffner, Craig. "Reverse Engineering a D-Link Backdoor" /dev/ttys0 (2013).

Vanderbeken, Eloi. "TCP/32764 backdoor, or how linksys saved Christmas!" GitHub (2013).

Authentication

Prompt

Success

Failure

Backdoor e.g. strcmp()

Hard to find.

Missing!
Our Solution: Input Determinism
Prompt

Authentication

Backdoor e.g. strcmp()

Success

Failure

Hard to find.

Easier to find!
Prompt

Backdoor e.g. strcmp()

Authentication

Success

Failure

Required input?

→ Indeterminable
Required input?

➔ Determinable!

Prompt

Backdoor e.g. strcmp()
Prompt

Backdoor e.g. strcmp()

Authentication

Success

Failure

Easier to find, but how?

Hard to find.
Security Policies
Security Policy

1. Identifies sensitive firmware functionality.
2. "By which point must a user be authenticated?"
3. Description of a logical property of the program.
Firmalice
Inputs:

➔ Firmware Sample
➔ Security Policy

Challenges:

➔ Large binary programs
➔ Unrelated user input

Analysis Steps:

➔ Static Analysis (backwards program slicing)
➔ Dynamic Symbolic Execution
➔ Authentication Bypass Check
Static Analysis
Dynamic Symbolic Execution
Authentication

Initial Stage

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prompt

Backdoor strcmp()

Authentication

Success

Step 1
Prompt

Backdoor strcmp()

Authenticated Paths

ID

Step 3

Authentication

Success
Prompt

Authentication

Backdoor strcmp()

Success

Step 4

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Prompt

Backdoor strcmp()

Authentication

Success

Step 5
Prompt

Backdoor strcmp()

Authentication

ID | Authenticated Paths
---|-------------------
   |                   

Success

Step 6
Prompt

Backdoor strcmp()

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
</tbody>
</table>

Step 7
Prompt

Authenticated Paths

ID | Authenticated Paths
---|-------------------
1  | Path 1

Backdoor

strcmp()

Success
Prompt

Authenticated Paths
1 Path 1

Backdoor strcmp()

Success

Step 8
Prompt

Authentication

Backdoor strcmp()

Success

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
</tbody>
</table>

Step 9
Prompt

Authentication

Backdoor strcmp()

Success

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
</tbody>
</table>

*Step 10*
Prompt

Authentication

Backdoor strcmp()

Success

ID | Authenticated Paths
---|-------------------
1  | Path 1
Prompt

Authentication

Backdoor strcmp()

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
</tbody>
</table>

Success

Step 12
Prompt

Authentication

Backdoor strcmp()

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
</tbody>
</table>

Success

Step 13
Prompt

Authenticated Paths

ID
1. Path 1
2. Path 2

Step 14
Prompt

Authentication

Backdoor strcmp()
Step 15

Prompt

Authentication

Backdoor strcmp()

Success

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
<tr>
<td>2</td>
<td>Path 2</td>
</tr>
</tbody>
</table>
Prompt

Authentication

Backdoor strcmp()

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
<tr>
<td>2</td>
<td>Path 2</td>
</tr>
</tbody>
</table>

Success

Step 16
Prompt

Authentication

Backdoor `strcmp()`

Authenticated Paths

<table>
<thead>
<tr>
<th>ID</th>
<th>Authenticated Paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Path 1</td>
</tr>
<tr>
<td>2</td>
<td>Path 2</td>
</tr>
<tr>
<td>3</td>
<td>Path 3</td>
</tr>
</tbody>
</table>

Success

Step 18
Authentication Bypass
Path 1

input == ???

Path 2

input == ???

Path 3

input == "..."
Implementation Details
VEX (Valgrind IR)

PyVEX

angr
Backdoor Example
3S Vision N5072

Linux embedded device.

HTTP server for management and video monitoring.

Security Policy

- Authentication required for footage access
- "Image-Type" header

Backdoor

- Hard-coded user credentials
- Username: 3sadmin
- Password: 27988303
Summary

➔ New backdoor model: *input determinism*

➔ Implemented analysis system

➔ Found backdoors in real firmware!
Prompt

... Authentication ...

Backdoor strcmp()

Success

Failure

Slicing with CFG
Dell 1130n

Modified VxWorks system.

Includes an SNMP daemon for monitoring and management.

Security Policy

➔ Manually identified sensitive memory regions

Backdoor

➔ Specific SNMPv1 community string would allow configuration without checking authentication

Slicing

➔ 14m
➔ 532 bb

DSE

➔ >11h