Forensic analysis of consumer routers

Esan Wit & Kim van Erkelens

April 11, 2014

1 Introduction

Many consumers have a router deployed at home in addition to the one provided by most ISPs. These routers often fulfil an important role within the local network architecture and as such contains a lot of information. This information may include devices previously attached to the network, traffic information, and usage patterns. Modern routers often come with a range of extra options which include features such as file sharing or DNS. Some parts of the information may be extracted or accessible via available interfaces or contained in inaccessible areas of the device.

2 Research question

The research question for this project is: How can forensic analysis be conducted on the Netgear WNDR3700 consumer router?

In order to answer this question the following sub-questions are set:

1. What are the different sources of information present on the router and how can they be accessed?

2. What is the volatility of these data?

3. What can be concluded from the data and what can it prove?

3 Scope

The experiments will be performed only on the newest firmware version available for the router. We are not going to investigate brute forcing the management password. We assume the presence of a default username and password, or the possibility of obtaining this from the suspect’s computer or (written) notes. However, we could test the effect of such an attack on data in memory.

4 Methodology

We start with a literature study towards forensic data acquisition. Based on this study we will identify data of interest for forensics that may be present on the router. For generating and extracting data, and testing its volatility, we will setup a test environment containing the router and a couple of attached devices. In order to achieve a consistent state of the router when performing the experiments multiple times, the behaviour of these devices will be automated.
5 Needed resources

This project has several requirements:

- Netgear WNDR3700
- JTAG connector
- USB drive

6 Planning

This planning of this project runs from the 14th of April till the 23rd of May.

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14-04</td>
<td>Literature research and setting up interface to device.</td>
</tr>
<tr>
<td>2</td>
<td>21-04</td>
<td>Extract data from device and analysis of extracted data.</td>
</tr>
<tr>
<td>3</td>
<td>5-05</td>
<td>Analysis of extracted data.</td>
</tr>
<tr>
<td>4</td>
<td>12-05</td>
<td>Final research, start creating report and presentation.</td>
</tr>
<tr>
<td>5</td>
<td>19-05</td>
<td>Finish presentation and report.</td>
</tr>
</tbody>
</table>

7 Previous research

Consumer routers are a small topic of research in the area of router forensics. Different approaches for acquiring data from consumer routers are described in previous research. A router has several interfaces through which data can be accessed. The easiest to access interfaces are the management web interface and telnet or SSH, which can be accessed via the router’s Ethernet port. However, issuing commands on the router may alter its memory. A method for acquiring memory uses the Joint Test Action Group (JTAG) [1] interface. This interface is often present in embedded devices and allows for direct access of the device’s memory. A drawback of JTAG is that it’s slow compared to the other methods [2].

Previous research by Fiebig into analysis of DHCP data available on home routers[3]. The research demonstrates a method for imaging the device memory and the extraction of DHCP information. It proposes further research into incorporating additional information from other services provided by the router. With our research we want to expand on this by investigating these additional services that are present on modern routers, and perform the research on another popular router that isn’t investigated before.

References

