Owning Your Home Network: Router Security Revisited

Marcus Niemietz, Jörg Schwenk
{marcus.niemietz, joerg.schwenk} @rub.de
Ruhr University Bochum
Table of Contents

1. Introduction
2. Web Attacker
3. Generalization
4. Default Configuration
5. Web Attacks
6. Fingerprinting
7. Countermeasures
8. Conclusions
Introduction

• Routers: center of private home networks
• Web stores like Amazon offer them for <$20
  – No keys and no displays
  – Web interface
• Our paper:
  Web-based attacks against these interfaces
  – Change critical settings
Introduction

• Methodology
  – 10 most popular routers from Amazon
    • TP-Link, Netgear, Buffalo, ...
  – Default configuration evaluated
  – UI redressing, Cross-Site Scripting, SSL/TLS
  – Fingerprinting possibilities analyzed
  – Countermeasures analyzed
Web Attacker

- Sets up a website → lures the victim to this site
- Arbitrary JavaScript code may be executed
- May send requests and may use scripts
Generalization

• Conditions
  – Web interface
  – Connected pointing device (e.g., mouse)

• Routers, network switches, smart TV systems, and network attached storage devices

• Router: Widely used, complex, important functionalities
# Default Configuration

<table>
<thead>
<tr>
<th>Router</th>
<th>Method</th>
<th>Username</th>
<th>Password</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-Link WR841N</td>
<td>BA</td>
<td>admin</td>
<td>admin</td>
<td><a href="http://192.168.0.1">http://192.168.0.1</a></td>
</tr>
<tr>
<td>Netgear N150</td>
<td>BA</td>
<td>admin</td>
<td>password</td>
<td><a href="http://192.168.1.1">http://192.168.1.1</a></td>
</tr>
<tr>
<td>Huawei E5331</td>
<td>Web</td>
<td>admin</td>
<td>admin</td>
<td><a href="http://192.168.1.1">http://192.168.1.1</a></td>
</tr>
<tr>
<td>D-Link DIR-615</td>
<td>Web</td>
<td>admin</td>
<td>(empty)</td>
<td><a href="http://192.168.0.1">http://192.168.0.1</a></td>
</tr>
<tr>
<td>Linksys WRT54GL</td>
<td>BA</td>
<td>(empty)</td>
<td>admin</td>
<td><a href="http://192.168.1.1">http://192.168.1.1</a></td>
</tr>
<tr>
<td>LogiLink WL0083</td>
<td>BA</td>
<td>admin</td>
<td>admin</td>
<td><a href="http://192.168.2.1">http://192.168.2.1</a></td>
</tr>
<tr>
<td>Belkin F7D4301</td>
<td>Web</td>
<td>–</td>
<td>(empty)</td>
<td><a href="http://192.168.2.1">http://192.168.2.1</a></td>
</tr>
<tr>
<td>Buffalo WCR-GN</td>
<td>BA</td>
<td>root</td>
<td>(empty)</td>
<td><a href="http://192.168.11.1">http://192.168.11.1</a></td>
</tr>
<tr>
<td>Fritz!Box 2170</td>
<td>Web</td>
<td>–</td>
<td>–</td>
<td><a href="http://192.168.178.1">http://192.168.178.1</a></td>
</tr>
<tr>
<td>Asus RT-N12</td>
<td>BA</td>
<td>admin</td>
<td>admin</td>
<td><a href="http://192.168.1.1">http://192.168.1.1</a></td>
</tr>
</tbody>
</table>
XSS, CSRF, UIR, and SSL/TLS

• XSS: Focus on reflected and stored XSS
  – Control the victim’s browser
• CSRF
  – Manipulate DNS settings
  – Change default passwords (D-Link DIR-615)
• UIR: Classic Clickjacking & Tabjacking
• SSL/TLS
UI Redressing
UI Redressing
UI Redressing
UI Redress
UI Redressing
UI Redressing

<h1>Funny pictures</h1>
<img src="lol.gif">
<button>Click me</button>
<img src="lol.gif">
<iframe style="position:absolute; z-index:1; opacity:0.0; filter:alpha(opacity=0); left:-120px; top:95px;" width="300" height="200" src="http://www.bing.com">
</iframe>
# Web Attacks

<table>
<thead>
<tr>
<th>Router</th>
<th>Version</th>
<th>UIR</th>
<th>XSS</th>
<th>TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-Link WR841N</td>
<td>3.13.27</td>
<td>✓</td>
<td>S</td>
<td>-</td>
</tr>
<tr>
<td>Netgear N150</td>
<td>1.0.2.54</td>
<td>✓</td>
<td>S</td>
<td>-</td>
</tr>
<tr>
<td>Huawei E5331</td>
<td>21.344.11</td>
<td>✓</td>
<td>-</td>
<td>(✓)</td>
</tr>
<tr>
<td>D-Link DIR-615</td>
<td>8.03</td>
<td>✓</td>
<td>S</td>
<td>-</td>
</tr>
<tr>
<td>Linksys WRT54GL</td>
<td>4.30.16</td>
<td>✓</td>
<td>S</td>
<td>(✓)</td>
</tr>
<tr>
<td>LogiLink WL0083</td>
<td>3.33.13</td>
<td>✓</td>
<td>R</td>
<td>-</td>
</tr>
<tr>
<td>Belkin F7D4301</td>
<td>1.00.25</td>
<td>✓</td>
<td>S</td>
<td>-</td>
</tr>
<tr>
<td>Buffalo WCR-GN</td>
<td>1.04</td>
<td>✓</td>
<td>R</td>
<td>-</td>
</tr>
<tr>
<td>Fritz!Box 2170</td>
<td>51.04.57</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Asus RT-N12</td>
<td>3.0.0.4.260</td>
<td>✓</td>
<td>R</td>
<td>-</td>
</tr>
</tbody>
</table>
UIR – Fritz!Box 2170

Kittens

Please drag and drop the kittens into the right box

Tired
Happy
Sad

More kittens
UIR – Fritz!Box 2170

<style>div, button { position:absolute; z-index:1; border:1px solid; pointer-events:none }</style>...

<img src="kitten-1.png" draggable="true"
ondragstart="event.dataTransfer.setData('text/plain','foobar')">...

<div style="top:35px; left:300px">Tired</div>...

<button style="top:195px; left:425px">More kittens</button>

<iframe src="http://192.168.178.1/cgi-bin/webcm?getpage=..."
Fingerprinting

• Get unique identifiers
  – HTTP Basic Authentication
    • WWW-Authenticate: Basic realm="VALUE"
  – Web Interface Authentication
    • HTTP resources
## Fingerprinting

<table>
<thead>
<tr>
<th>Router</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TP-Link WR841N</td>
<td>TP-LINK Wireless N Router WR841N</td>
</tr>
<tr>
<td>Netgear N150</td>
<td>NETGEAR WNR1000v3</td>
</tr>
<tr>
<td>Linksys WRT54GL</td>
<td>WRT54GL</td>
</tr>
<tr>
<td>LogiLink WL0083</td>
<td>Portable Wireless AP/Router</td>
</tr>
<tr>
<td>Buffalo WCR-GN</td>
<td>AirStation: Enter ”root” for user name.</td>
</tr>
<tr>
<td>Asus RT-N12</td>
<td>RT-N12</td>
</tr>
</tbody>
</table>
Fingerprinting

• Huawei E5331

• D-Link DIR-615

• Fritz!Box 2170

• Belkin F7D4301
Countermeasures

• Randomization of the default login data
Countermeasures

• Minimize Information Leakage
  – "TP-Link WR841N" ➔ "Router Login XXX"

• SSL/TLS

• Input Validation

• X-Frame-Options

• Window name
  – window.name="TOKEN"

• Cookie flags: $httpOnly$ and secure
Conclusions

• Representative overview of the security of current home router Web interfaces
• All 10 Web interfaces are vulnerable
• Well-known countermeasures like X-Frame-Options are not implemented
Thank you for your attention. Questions?