Binary Scanning: The First Line of Defense Against Security Breaches

October 11, 2017

Tae-Jin (TJ) Kang
CEO & President, insignary
Know What’s In Your Third Party Code
Why Use Third Party Code?

• To quickly build on sophisticated components or technology platforms
• To increase efficiency and reduce costs
Concerns about Third Party Code
Open Source Prevalence & Vulnerabilities

96% of scanned applications included Open Source components

67% of analyzed applications using Open Source components had vulnerabilities

50% of vulnerabilities found in analyzed applications ranked “HIGH SEVERITY”

References: Black Duck’s 2017 Open Source Security and Risk Analysis audit
# About Security Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>Heartbleed</th>
<th>Shellshock</th>
<th>Freak</th>
<th>Ghost</th>
<th>DROWN</th>
<th>SambaCry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>OpenSSL</td>
<td>Bash</td>
<td>OpenSSL</td>
<td>GNU C Library</td>
<td>OpenSSL</td>
<td>SAMBA</td>
</tr>
</tbody>
</table>

## Graphical Representation

![Graph showing security vulnerabilities over time](image-url)

- **Heartbleed**: 2014
- **Shellshock**: 1989
- **Freak**: 1990s
- **Ghost**: 2000
- **DROWN**: 1990s
- **SambaCry**: 1990s

### Vulnerability Counts

<table>
<thead>
<tr>
<th>Year</th>
<th>Heartbleed</th>
<th>Shellshock</th>
<th>Freak</th>
<th>Ghost</th>
<th>DROWN</th>
<th>SambaCry</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>4,931</td>
<td>6,608</td>
<td>5,632</td>
<td>5,732</td>
<td>4,639</td>
<td>5,288</td>
</tr>
<tr>
<td>2006</td>
<td>6,608</td>
<td>6,514</td>
<td>5,632</td>
<td>5,732</td>
<td>4,639</td>
<td>5,288</td>
</tr>
<tr>
<td>2007</td>
<td>6,608</td>
<td>6,514</td>
<td>5,632</td>
<td>5,732</td>
<td>4,639</td>
<td>5,288</td>
</tr>
<tr>
<td>2008</td>
<td>6,514</td>
<td>6,514</td>
<td>5,632</td>
<td>5,732</td>
<td>4,639</td>
<td>5,288</td>
</tr>
<tr>
<td>2009</td>
<td>5,632</td>
<td>5,632</td>
<td>5,732</td>
<td>4,639</td>
<td>4,150</td>
<td>5,186</td>
</tr>
<tr>
<td>2010</td>
<td>5,732</td>
<td>5,732</td>
<td>4,639</td>
<td>4,150</td>
<td>5,288</td>
<td>5,186</td>
</tr>
<tr>
<td>2011</td>
<td>4,639</td>
<td>4,150</td>
<td>4,639</td>
<td>5,288</td>
<td>5,186</td>
<td>7,937</td>
</tr>
<tr>
<td>2012</td>
<td>4,150</td>
<td>4,639</td>
<td>5,288</td>
<td>5,186</td>
<td>7,937</td>
<td>6,488</td>
</tr>
<tr>
<td>2013</td>
<td>5,288</td>
<td>5,186</td>
<td>7,937</td>
<td>6,488</td>
<td>5,267</td>
<td>5,267</td>
</tr>
<tr>
<td>2014</td>
<td>5,186</td>
<td>7,937</td>
<td>6,488</td>
<td>5,267</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>6,488</td>
<td>5,267</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>5,267</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Equifax – A Preventable Breach

Exploited Known Security Vulnerability in Apache Struts

<table>
<thead>
<tr>
<th></th>
<th>Heartbleed</th>
<th>Shellshock</th>
<th>Freak</th>
<th>Ghost</th>
<th>DROWN</th>
<th>SambaCry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>OpenSSL</td>
<td>Bash</td>
<td>OpenSSL</td>
<td>GNU C Library</td>
<td>OpenSSL</td>
<td>SAMBA</td>
</tr>
</tbody>
</table>

First discovered patch update in March

60 days to fix

Breach occurred in mid-May to July

Personal data of **145.5 million** individuals exposed
Binary Scanning
As The First Line of Defense
Binary Scanning Tools

1. Static Code Analyzers
2. Checksum-Based Code Scanners
3. Hash-Based Code Scanners
4. Fingerprint-Based Code Scanners
Static Code Analyzers

• Designed to analyze source code to find common programming errors, such as buffer overflows and SQL Injection Flaws

• Offers limited binary code analysis by disassembling binary code to obtain source code
  • Potential violation of intellectual property laws
Checksum and Hash Based Scanners

- Checksum-Based
  - Does not work with modified code
- Checksum & Hash-Based
  - Limited databases of OSS components
    - Dependency on CPU architecture
Fingerprint-based Binary Code Scanners

• Based on Binary Analysis Tool (BAT)
• Independent of CPU architecture
• Use fingerprints based on identifiers such as strings, function, or variable names extracted from source code or binary code
• Increase fidelity by using other information such as file names and package databases
GENIVI Code & Specific Component Scanning Results
GENIVI App Scan Results

Scan Results Summary View: libvsi-core.so

<table>
<thead>
<tr>
<th>File name</th>
<th>Component</th>
<th>Security Risks</th>
<th>Licenses</th>
<th>Litigator code</th>
</tr>
</thead>
<tbody>
<tr>
<td>libvsi-core.so</td>
<td>vehicle-signal-interface</td>
<td>-</td>
<td>MPL, MPLv2</td>
<td>-</td>
</tr>
</tbody>
</table>

Detected GENIVI component
Detected GENIVI specific component

Dbus component provides
- D-Bus daemon
- D-Bus libraries

At least 1.4 implementation version* required

*GENIVI Platform Compliance Specification
Thank you!

Please visit our showcase between 5:30PM and 8:30PM today

Scan the QR code to test your binary at

www.truthisinthebinary.com

GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries.
Copyright © GENIVI Alliance 2017.