**Overview**

**Goals of BlackBox**

1. Log the pivotal control flow events of a successful exploit.
2. Block future attempts at exploiting a known program vulnerability.

**Basic Approach**

1. Learn normal program behavior during offline profiling.
2. Monitor programs online using binary translation (DynamoRO).
3. Filter out normal program behavior and highlight unusual behavior.

**Why Security Auditing?**

Automated security continues to face challenges, e.g. ROP:

1. Stack guards and stack shields can be bypassed.
2. COTS rewriting approaches can be defeated by crafted gadgets.
3. Compilers cannot easily compute all return targets.

A Microsoft media licensing module uses non-conventional returns to enter dynamically generated code during startup of Word.

**The Details**

**Log Filter**

- Trusted Trace
- Log Filter
- Trusted Profile

**Program Events**

1. Shtastically Compiled Code
2. Shadow Stack
3. Dynamically Generated Code
4. Blacklist

**Performance**

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>BlackBox Offline</th>
<th>BlackBox Online</th>
<th>BlackBox Remote</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome</td>
<td>1.2%</td>
<td>1.1%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Adobe PDF</td>
<td>1.3%</td>
<td>1.2%</td>
<td>1.4%</td>
</tr>
<tr>
<td>Word</td>
<td>1.1%</td>
<td>1.0%</td>
<td>1.2%</td>
</tr>
<tr>
<td>Excel</td>
<td>1.4%</td>
<td>1.3%</td>
<td>1.5%</td>
</tr>
<tr>
<td>Outlook</td>
<td>1.2%</td>
<td>1.1%</td>
<td>1.3%</td>
</tr>
<tr>
<td>Adrenalin</td>
<td>1.5%</td>
<td>1.4%</td>
<td>1.6%</td>
</tr>
</tbody>
</table>

**BlackBox**

A Microsoft media licensing module uses non-conventional returns to enter dynamically generated code during startup of Word.

Trust BlackBox as a trusted module and generate helper function for use with dynamically generated code.

JIT code varies across execution due to various random factors. BlackBox abstracts JIT monitoring to the API level.

**Forwards**

1. Trusted Branches
2. Non-Conventional Returns
3. Shadow Stack
4. Code Generator

**Copyright**

Copyright 2014 Byron Hawkins and Brian Demsky, University of California, Irvine, USA. All rights reserved.

**Acknowledgments**

BlackBox is supported by the NSF under award 1228992, grants CCF-0846195, CCF-1217854, CNS-1228995, and CCF-1319786; and by the Center for Future Architectures Research (C-FAR).