EPOXY – Enabling Robust Protections for Bare-metal Systems
Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer

Bare-metal?
A system without an OS
Examples:
• Amazon Dash Button
• Controller in SD Cards
• Smart Locks
• WiFi SoC’s
Increasingly connected
Security is critical

Default: No Defenses

Security Hardware
Sensitive IO
IO
Global Data
Stack
Code

Only Root Level Execution

Defense Challenges
No separate privileges
• Single application
• No higher privileged software
Small memories
• 1KB - 2MB of Flash
• 1KB - 512KB RAM
No virtual memory
Run-time constraints
Low power constraints

Techniques
Privilege Overlay
• Uses static analysis to create privileged and unprivileged execution
• Foundation for other defenses
Enable Memory Protection
• Provides DEP
• Code Integrity
SafeStack2 and Diversity
• Protects against ROP attacks
• Protects global data

Our Solution – EPOXY1

EPOXY
LLVM-based compiler

Hardened Application

Security Hardware
Sensitive IO
IO
UnSafeStack
Global Data
Reg Stack
Code

Privilege Execution
Unprivileged Execution

Non-writable ROP protection via diversification

RAM – No Execute ROP Protections
Stack Smashing Defenses
Isolated “Unsafe” Locals
Access Restricted
Enabled Access Restricted

Security Analysis
ROP gadgets survival

<table>
<thead>
<tr>
<th>App</th>
<th>Total</th>
<th>2</th>
<th>5</th>
<th>25</th>
<th>50</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>PinLock</td>
<td>294K</td>
<td>14K</td>
<td>8K</td>
<td>313</td>
<td>0</td>
<td>48</td>
</tr>
<tr>
<td>FatFs</td>
<td>1,009K</td>
<td>39K</td>
<td>9K</td>
<td>39</td>
<td>0</td>
<td>32</td>
</tr>
<tr>
<td>TCPEcho</td>
<td>676K</td>
<td>22K</td>
<td>9K</td>
<td>985</td>
<td>700</td>
<td>107</td>
</tr>
</tbody>
</table>

Comparison to FreeRTOS-MPU

EPOXY

PinLock

RTOS

FatFs

TCP Echo

---|-----------|----------|------------|------------
PinLock | EPOXY | 16 | 2 | 823K | 1.4K
RTOS | 44 | 30 | 823K | 813K
FatFs | EPOXY | 27 | 12 | 33.3M | 3.9K
RTOS | 58 | 14 | 34.1M | 33.0M
TCP Echo | EPOXY | 43 | 35 | 310M | 1.5K
RTOS | 74 | 51 | 322M | 307.0M

Performance

Memory Overhead (Bytes)

<table>
<thead>
<tr>
<th>App</th>
<th>Code</th>
<th>Global Data</th>
<th>Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>PinLock</td>
<td>3,390</td>
<td>14.6</td>
<td>104</td>
</tr>
<tr>
<td>FatFs</td>
<td>2,839</td>
<td>18.2</td>
<td>164</td>
</tr>
<tr>
<td>TCPEcho</td>
<td>3,249</td>
<td>7.2</td>
<td>128</td>
</tr>
</tbody>
</table>

References

Acknowledgments
Partially funded under National Science Foundation Grant Numbers CNS-1441555 and CNS-1348114. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Also funded by Sandia National Laboratories, a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.