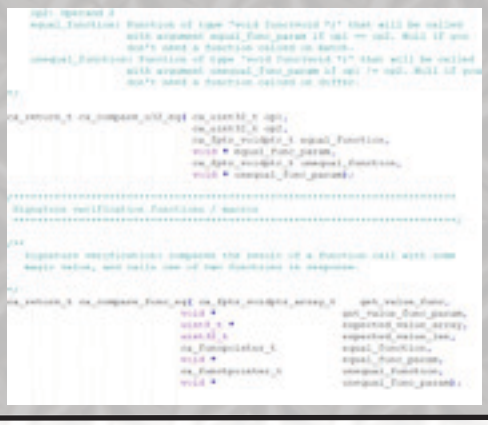
ChipArmour®

NewAE Technology
Embedded security arsonists.

Fault-Injection Resistant Software Library.

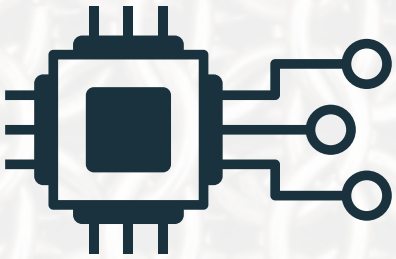
Eine Fault-Injection Attacke ermöglicht es einem Angreifer, ansonsten sichere Systeme, zu kompromittieren. Angreifer, die physischen Zugriff auf Ihr System haben, können erreichen, dass einzelne Instruktionen im Code übersprungen werden. Dies kann dazu führen, dass Operationen, die für einen sicheren Bootvorgang nötig sind, niemals ausgeführt bzw. validiert werden.

NewAe Technology Inc. ist der erste Anbieter von frei verfügbaren und kommerziellen Werkzeugen für Fault Injection Angriffe, einschließlich Voltage Fault Injection und Electromagnetic Fault Injection (EMFI). Diese Werkzeuge wurden von unseren Kunden mehrfach erfolgreich benutzt, um Schwachstellen in ihren Produkten zu erkennen und nachzuvollziehen.



Die ChipArmour Bibliothek bietet Fault-Injection resistente Funktionen um Aufgaben, wie die Validierung eines sicheren Boot-Images oder den Vergleich geheimer Werte, durchzuführen. Integrierte Validierungsbeispiele können verwendet werden, um Ihren bestehenden Code mit dem ChipArmour gehärteten Code zu vergleichen. So lässt sich das erweiterte Schutzniveau, das die ChipArmour-Bibliothek bietet, anzeigen und vergleichen.

ChipArmour ist open-source und unter der permissiven Apache-Lizenz lizensiert. ChipArmour kann kostenlos genutzt werden, kommerzieller Support ist direkt bei NewAe Technology Inc. verfügbar. NewAe Technology Inc. bietet auch eine kommerzielle Version mit robusten Prüfständen, basierend auf echter Hardware, an um jedes Kompillierungsergebnis auf Fault Injection Resistenz zu prüfen.



ChipArmour.com

NewAE Technology Inc.
1083 Queen St., Suite 196
Halifax, NS. B3H 2R8
Canada