開発テーマ名

Super Creator

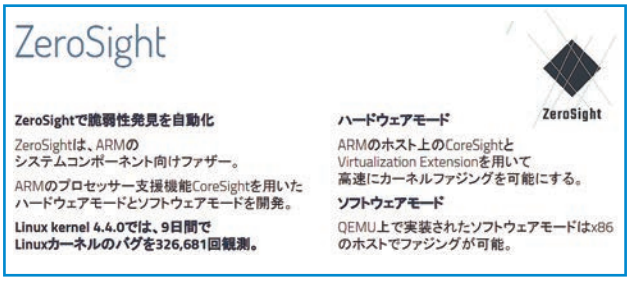
プロセッサトレースを用いた組み込みデバイス向けファザーの開発

大塚　馨
おおつか　かおる

《略歴》
非公開

テーマ概要

脆弱性の発見は、これまで天才ハッカーに頼るところが大きかったが、近年では入力空間を網羅的に探索して脆弱性を発見するファザー（Fuzzer）が普及しつつある。サーバやPCの多くはインテルプロセッサが使用されており、従来のファザー研究もインテル製プロセッサを前提とするものが多い。しかし、近年ではスマートフォンやIoT機器の普及で、ARMプロセッサが使用された機器の脆弱性検査ニーズが高まっている。そこで、本プロジェクトではARMプロセッサ向けファザー「ZeroSight」の開発を行った。ARMのハードウェアトレース機能「CoreSight」を利用すべく7種のボードを試したがいずれも不具合があり、 QEMUを用いたソフトウェアトレース機能に差し替えて実現した。ARM版Linuxカーネルに適用した結果、326,881個のバグを自動検出し、このうち10,781個はクラッシュを誘発、69種の異なる基本ブロックに含まれることを確認した。



首藤 PM の評価

ARMプロセッサ＆OSカーネル＆バイナリを対象にできる、必要性・緊急性が高い割にこれまで世界に存在しなかったファザー（ソフトウェアテストツール）を本当に作り上げてしまった。加えて、それを使ってLinuxカーネルのバグをもりもりと発見し始めた。大塚君の成果によって、世界はより安全になる。大塚君の情熱と好奇心、また、それらによって培われたのであろう人並外れた技術が、この成果を可能にした。非常に高い技術を要する開発を完遂したというだけでなく、ハード入手不可という困難をエミュレーションで乗り切ったことにも驚かされた。世界初の、社会的インパクトも大きい成果であり、文句なしにスーパークリエータである。

近況メッセージ

・開発成果の近況、展開方針、今後の目的など

ファジングに利用できるARMハードウェアトレース機能「CoreSight」が完動するボードの探索を続け、引き続き高速化の可能性を探る。また、 ファジングの高速化に本質的に寄与するミューテーションアルゴリズムについて、Deep Learning等の機械学習手法を取り入れる方向で研究を進める。今回の開発成果は、未踏OBの木村廉氏が起業した株式会社リチェルカセキュリティが提供する脆弱性検査ツールに採用される予定である。

・近況

未踏同期/OBの先輩やPMの先生方の支援はとても厚く、未踏プロジェクトを通して他では得がたい大変貴重な体験をさせて頂いた。株式会社リチェルカセキュリティのリサーチャーも拝命して、未踏プロジェクト「ZeroSight」で開発した成果を元に、組込み機器のセキュリティ向上にも貢献して行ければと考えている。当面は勉強に集中して基礎をしっかり学び、将来、新しい学問や研究に取り組める力を養いたいと思っている。