IPA

2016 年度　未踏 IT 人材発掘・育成事業　採択案件評価書

1. 担当 PM

後藤 真孝 PM（産業技術総合研究所 情報技術研究部門 首席研究員）

2. 採択者氏名

クリエータ：木村 廉（神戸大学 工学部 情報知能工学科）

3. 委託金支払額

2,304,000 円

4. テーマ名

カーネルソフトウェア開発支援ツール

5. 関連 Web サイト

https://github.com/KernelAnalysisPlatform/

6. テーマ概要

本プロジェクトでは、デバイスドライバなどのカーネル空間で動作するソフトウェアの開発を支援するためのカーネルソフトウェア開発支援ツール「Kernel Analysis Platform」を開発した。このツールは、開発者が利用するユーザインタフェースであるフロントエンドと、カーネルソフトウェアの動作情報を記録する基盤技術であるバックエンドで構成され、後者によって前者の動作が可能になる。前者のフロントエンドとしては、カーネルソフトウェア専用のデバッガ「KlareDbg」および自動テストツール「kvalgrind」の二つを開発した。さらに後者のバックエンドとして、仮想マシン（VM）で OS ごとエミュレートさせる方式で実装した「QEMU 改」と，ハイパーバイザにより実機を利用しつつ解析対象のカーネルソフトウェアのみエミュレート（インタプリタ実行）させる方式で実装した「K2E」の二つを開発した。フロントエンドの二つとバックエンドの二つは、必要に応じて自由に組み合わせて利用でき、これによりカーネルソフトウェアのデバッグ効率が向上した。

7. 採択理由

ソフトウェア開発においてデバッグは不可欠だが、デバイスドライバなどのカーネル空間で動作するソフトウェアのデバッグの場合には、通常のユーザ空間でのデバッグを効率化する動的解析ツールの利用が困難という問題があるため、それを解決するカーネルソフトウェア開発支援ツールを開発する提案である。そのために、ターゲットとなる OS を CPU エミュレータ上で動作させ、デバッグ対象のカーネルソフトウェアのバイナリコードを CPU エミュレータが中間表現に変換して実行する際に、その中間表現に様々なデバッグ用コードを挿入する。これにより動的に詳細な情報を把握することが可能となり、さらに開発者が使いやすいユーザインタフェースも提供することで、柔軟で効率的なデバッグを実現することができる点が優れている。

木村君は、低レイヤーのシステムソフトウェア開発に興味を持つ人たちがもっと増えて欲しいという情熱を持っており、既に自身も様々な形でその開発に取り組んでオープンソースソフトウェア（OSS）に貢献してきている点が素晴らしい。既にオープンソースの CPU エミュレータ「QEMU」の内部構造における主要範囲をソースコードレベルで理解しており、ソフトウェアのバイナリコードあるいは中間表現にコードを挿入して動的解析する手法 DBI（Dynamic Binary Instrumentation）を QEMU 上で実現する方法に関しても、QEMU をベースとした DECAF へのパッチコミットを通じて熟知している。その木村君の情熱と高い能力を活かして、大きなインパクトをもたらす成果を創出できるように、提案内容だけで満足せずに広い視野で様々な挑戦をしてくれることを期待したい。

8. 開発目標

ソフトウェア開発においてデバッグは不可欠だが、デバイスドライバなどのカーネル空間で動作するソフトウェアのデバッグの場合には、通常のユーザ空間でのデバッグを効率化する動的解析ツールの利用が困難という問題があるため、それをカーネルソフトウェア開発支援ツールの開発によって解決することを目標とした。そのために、ターゲットとなる OS を CPU エミュレータ上で動作させ、デバッグ対象のカーネルソフトウェアのバイナリコードを CPU エミュレータが中間表現に変換して実行する際に、その中間表現に様々なデバッグ用コードを挿入する計画を立てた。これにより動的に詳細な情報を把握することが可能となり、さらに開発者が使いやすいユーザインタフェースも提供することで、柔軟で効率的なデバッグを実現することを目指した。

9. 進捗概要

未踏プロジェクト開始時点で、木村君は既に、QEMU の主要ソースコードを読解し、デバイスドライバデバッグのバックエンドに位置づけられる QEMU 改の実装に着手するなど、本気で取り組んでいた。プロジェクト開始後、フロントエンドに位置づけられるデバッガの KlareDbg や自動テストツールの kvalgrind の開発にも着手し、KlareDbg については早々にプロトタイプを完成させて着実にプロジェクトを進めていた。

10 月に現場レビューをした際には、実装に関しては既に進んできているため、デバッグ体験の未来、デバッグコミュニティの未来を創るアイディアも含め、さまざまな方向性での発展的な開発内容について議論を深めることができた。また、プロジェクトを進める上での優先順位やハードルについて議論した。

11 月の八合目会議（中間合宿）では、バックエンドの QEMU 改の実装が完了し、そのフロントエンドの KlareDbg や kvalgrind についても機能を段階的に実装して、デモが可能な状態となっていた。しかし、QEMU に基づく実装ではフルエミュレーションのために実行速度の低下がひどく、しかも QEMU がエミュレートできる仮想ハードウェアのドライバにしか対応できないという弱点を持っていた。そこで木村君は当初のプロジェクトの想定を超えて、QEMU を用いない、新たなハイパーバイザを使ったバックエンドの開発を自ら提案し、その開発に着手していた。そこで、開発と平行して、この価値や意義を一般の人々に的確に伝えるプレゼンを木村君自身ができるように、さまざまなアドバイスをした。

1 月の進捗ミーティングでは、順調に実装が進んでいたことから、技術的ないくつかのゴールを改めて整理した上で、いかにこの価値を伝えるかという課題に時間を割いて指導した。そして、成果報告会での発表スライドのドラフトに対し、ストーリーを明確化し、成果の魅力がどうすればより伝わるかについて議論した。

2 月の成果報告会では、「カーネルソフトウェア開発支援ツール」について極めてわかりやすく説明し、デバイスドライバのデバッグのための KlareDbg と kvalgrind の二つのフロントエンドが、バックエンドとしてエミュレーションベースの QEMU 改とハイパーバイザーベースの K2E の両方と使えることをデモ動画も交えて具体的に紹介しながら魅力的な成果を見事に発表した。

10. プロジェクト評価

デバイスドライバなどのカーネル空間で動作するソフトウェアの開発を支援するためのカーネルソフトウェア開発支援ツール「Kernel Analysis Platform」を木村君は実現した。ソフトウェア開発においてデバッグは不可欠だが、カー

ネルソフトウェアのデバッグの場合には、通常のユーザ空間でのデバッグを効率化する動的解析ツールの利用が困難という問題があった。木村君は、この問題を解決するために、開発者が利用するユーザインタフェースであるフロントエンドと、カーネルソフトウェアの動作情報を記録する基盤技術であるバックエンドで構成される「Kernel Analysis Platform」を実現することに成功した。フロントエンドとしては、カーネルソフトウェア専用のデバッガ「KlareDbg」および自動テストツール「kvalgrind」の二つを開発した。特に KlareDbg では、従来はユーザ空間でのデバッグにしか用いられていなかった Timeless Debugging というデバッグ手法を実装することで、任意の命令に自在にカーソルを移動して実行時の状態を復元・確認可能にした点が優れている。さらにバックエンドでは、当初の計画では、仮想マシン（VM）で OS ごとエミュレートさせる「QEMU 改」のみの開発であったにも関わらず、実機を用いた効率的なデバッグも可能にした方が開発者の利便性が高いことから、ハイパーバイザにより実機を利用しつつ解析対象のカーネルソフトウェアのみエミュレート（インタプリタ実行）させる「K2E」も木村君は開発した。しかも K2E では、開発者が容易にテストを拡張できるようにプラグイン機構を提供し、そのプラグイン開発を円滑にできるように、C++の標準ライブラリまで自力で全て移植してしまうなど、非常に大規模なソフトウェア開発を木村君は成し遂げた。VM には QEMU、ハイパーバイザには BitVisor という既存の優れたソフトウェアをベースにしながら、木村君自身がそれらのソフトウェアを読解して深く理解することで、従来は実現されていなかった改造・拡張を可能にして二つのバックエンドを実現したことは、当初の想定を大きく上回る特筆すべき成果である。既に GitHub にて一般公開中であり、フィードバックを得ながら開発を進めるなど、カーネルソフトウェア開発を的確に支援する素晴らしい成果をあげた。

11．今後の課題

既に優れた成果を創出しているが、今後は、バックエンドの K2E 等の完成度をさらに高めていくことが課題である。また、フロントエンドを木村君自身もさまざまなカーネルソフトウェア開発に活用していくことで、ユーザインタフェース等のユーザビリティをさらに向上していく課題も残されている。