

成果の概要

移動コードを基本とした セキュアなプログラミング言語処理系

研究代表者 米澤 明憲 (東京大学)

1 参加研究者

研究代表者

米澤 明憲 東京大学 大学院 情報学環 教授

研究分担者

田浦 健次郎 東京大学 大学院
情報理工学系研究科 助教授

増原 英彦 東京大学 大学院
総合文化研究科 助教授

住井 英二郎 東京大学 大学院
情報学環 助手

研究協力者

Benjamin ペンシルバニア大学 工学部
C. Pierce 計算機情報科学科 助教授

大岩 寛 東京大学 大学院
情報理工学系研究科

Reynald Affeldt 東京大学 大学院
情報理工学系研究科

前田 俊行 東京大学 大学院
情報理工学系研究科

WWW

<http://www.yl.is.s.u-tokyo.ac.jp/>

2 研究概要

現代のコンピュータにおいて、不正アクセスによる個人情報流出、サービス拒否攻撃による業務妨害、金融機関のシステム障害、個人用計

算機の不安定さといった問題は、ほぼすべてソフトウェアの欠陥が原因である。本研究班では、そのような欠陥を防止しやすい、安全なプログラミング言語について研究を推進している。特に、MLのような現代的な言語を様々な分野に適用するだけでなく、C, Java, Perl といった産業界で定着している古典的な言語についても、最新の理論を応用するための研究・開発を行っている。本年度の主要な成果を以下に挙げる。

2.1 安全な C 言語処理系 [発表 1, 発表 7, 発表 10]

昨年度に引き続き、バッファ溢れ等のセキュリティホールを防止するための、安全な C 言語処理系の研究・開発を進めている。具体的には、基本的な方式の提案と、プロトタイプによる実験の結果を論文誌 [発表 1] ならびに国際会議 [発表 7] で発表するとともに、メールサーバ (sendmail ないし qmail) や Web サーバ (apache) といった大規模なアプリケーションプログラムを実行するための、本格的な実装に取り組んでいる。また、オペレーティングシステムのシステムコールのような、外部のソフトウェアと我々の C 言語処理系との相互運用性を向上するために、データ表現の変換や事前条件の検査を行うコード (stub) を半自動的に生成するインターフェイス記述言語 (IDL) を設計・開発した [発表 10]。

2.2 ユーザプログラムをカーネルモードで実行可能な Linux[公開 1]

型検査等の実行前検証により安全性が事前に保証されているユーザプログラムを、カーネルモードで実行できる Linux (オープンソースの UNIX の一種) を開発・公開 [公開 1] した。この方式では、一般にハードウェアによる実行時検査の大半が不要となり、システムコールのオーバーヘッドが大幅に軽減する。基礎的な実験によれば、システムコール自体にかかるオーバーヘッドは、約 1 ミリ秒から 30 ナノ秒程度に減少した。これにより、データベースやネットワークサーバといった、入出力の頻繁なアプリケーションを高速化できる。現在は、より様々なプログラムで大規模な実験を行うために、標準ライブラリ (libc) を移植する作業を行っている。

2.3 文字列処理のための正規表現型 [発表 4, 発表 8]

Web サーバにおける CGI プログラムなどにおいては、文字列処理が重要な位置を占めることが多い。しかし、この処理は誤りが起きやすいにも関わらず、その正しさを確かめたり、バグを見つけるためのシステムはあまり考えられておらず、サイト間スクリプティング脆弱性によりパスワードやクレジットカード番号が漏洩するといった、重大なセキュリティホールの原因となっている。そこで、本研究では正規表現を文字列の型とみなして型検査や型推論を行うことにより、文字列処理の検証・解析を実現する。本年度の論文 [発表 4, 発表 8] では、型システムの基礎となる型付け規則と、部分的な型推論 (パターン変数のみ) の方式を提案し、それらの正当性を証明した。現在は、制約解消と文脈自由文法の正規表現近似にもとづき、パターン変数以外の変数の型も推論する方式について研究している。この型推論が実現すれば、本研究を応用した現実的な文字列処理言語を開発することも可能であると期待される。

2.4 安全なプログラミング言語の応用

ML や Scheme といった安全なプログラミング言語や、それらの言語における研究の成果を、Java [発表 2] や C++ [発表 3] といった従来の言語に適用したり、メールシステム [発表 6], 暗号プロトコル [発表 9], 移動コードによるパケットフィルタリング [発表 5], 対戦プログラム [特記 1] といった様々な領域の問題に応用し、そのような言語ないし研究が (従来の技術と比較しても) 有用であることを実証した。

3 今後の展望

来年度は、上述の方向性にしたがって各研究をさらに発展・推進し、特に

- 安全な C 言語処理系の完成
- より現実的・大規模なアプリケーションによるカーネルモード Linux の実験
- 正規表現型を実装した文字列処理言語の設計・開発

といった、本特定領域研究班による基礎研究を応用した成果の実現・公開を目指す。

4 平成 14 年度成果要覧

公開ソフトウェア

[公開 1] Kernel Mode Linux. Toshiyuki Maeda.
<http://www.y1.is.s.u-tokyo.ac.jp/~tosh/kml/>.

特記事項

[特記 1] 第 5 回 ICFP プログラミングコンテスト優勝. 大岩 寛, 住井 英二郎, 関口 龍郎.
2002 年 10 月. <http://icfpcontest.cse.ogi.edu/>.

発表論文

- [発表 1] 大岩 寛, 住井 英二郎, 米澤 明憲: 安全性を保証する ANSI-C 実行系の実装手法. コンピュータソフトウェア, 岩波書店, 19 巻 3 号 39–44 頁, 2002 年 5 月.
- [発表 2] Akihito Nagata, Eijiro Sumii, and Akinori Yonezawa: A Scheme-to-Java Translator with Soft Typing. Manuscript, May 31, 2002. 7 pages. <http://www.yl.is.s.u-tokyo.ac.jp/~sumii/pub/scm2java.ps.gz>.
- [発表 3] 増山 隆, 住井 英二郎, 米澤 明憲: C++ テンプレートを分割コンパイルするためのアプローチ. 情報処理学会第 39 回プログラミング研究会, 2002 年 6 月 17–18 日. 16 頁.
- [発表 4] Naoshi Tabuchi, Eijiro Sumii, and Akinori Yonezawa: Regular Expression Types for Strings in a Text Processing Language. Proceedings of Workshop on Types in Programming (TIP'02), Dagstuhl, Germany, July 9, 2002 (Electronic Notes in Theoretical Computer Science, Elsevier Science, the Netherlands, to appear). 19 pages.
- [発表 5] Eric Y. Chen, 柏 大, 富士 仁, 米澤 明憲: Moving Firewall における DDoS 攻撃対策システムの評価. 電子情報通信学会情報ネットワークシステム研究会予稿集, 信学技報, NS2002-121, 2002 年 9 月, pp. 73–78.
- [発表 6] Reynald Affeldt and Naoki Kobayashi: Formalization and Verification of a Mail Server in Coq. Proceedings of International Symposium on Software Security, Tokyo, Japan, November 8–10, 2002 (Software Security – Theories and Systems, Lecture Notes in Computer Science: Hot Topics, Springer-Verlag, Germany, vol. 2609). 17 pages.
- [発表 7] Yutaka Oiwa, Tatsuro Sekiguchi, Eijiro Sumii, and Akinori Yonezawa: Fail-Safe ANSI-C Compiler: An Approach to Making C Programs Secure (Progress Report). Proceedings of International Symposium on Software Security, Tokyo, Japan, November 8–10, 2002 (Software Security – Theories and Systems, Lecture Notes in Computer Science: Hot Topics, Springer-Verlag, Germany, vol. 2609). 21 pages.
- [発表 8] 田淵 直, 住井 英二郎, 米澤 明憲: テキスト処理言語における文字列のための正規表現型. 情報処理学会論文誌: プログラミング, 採録済. 12 頁.
- [発表 9] Eijiro Sumii and Benjamin C. Pierce: Logical Relations for Encryption. Journal of Computer Security, IOS Press, the Netherlands, to appear. 29 pages.
- [発表 10] 末永 幸平, 大岩 寛, 住井 英二郎, 米澤 明憲: Fail-Safe C のためのインターフェイス定義言語. 投稿中. 7 頁.