東北大学
TOHOKU UNIVERSITY

Press Release

2023 年 8 月 1 日

報道機関　各位

国立大学法人東北大学

コンピュータの秘密情報をスパイプログラムから守る新しい暗号化技術を開発
高セキュリティコンピュータの実現に向けて大きく前進

【発表のポイント】

- スパイプログラム（注 1）を用いたキャッシュサイドチャネル攻撃は、現代のコンピュータの動作原理に起因するセキュリティ上の脆弱性であり、対策技術の確立が急務となっていました。
- 同攻撃に対する有望な対策の一つであるキャッシュメモリ内のデータを暗号化する「キャッシュランダム化」を安全に運用するための条件と設計方針を定式化しました。
- キャッシュランダム化のための専用暗号技術「SCARF」を開発し、その性能と安全性を実証しました。
- 本成果は今後開発されるコンピュータの高セキュリティ化に貢献すると期待されます。

【概要】

現代のコンピュータは、よく使うデータを内部の小規模な高速メモリに格納して利用することで高速な処理を実現しています。一方でスパイプログラムと呼ばれる悪意あるプログラムを用いることで、この内部メモリのデータからユーザの秘密情報（パスワードや暗号鍵など）を盗み出すキャッシュサイドチャネル攻撃（注 2）の脅威が指摘されており、その対策が急務となっていました。

東北大学電気通信研究所の上野嶺助教は、日本電信電話株式会社社会情報研究所およびドイツ・ルール大学ボーフム（RUB）の Cyber Security in the Age of Large-Scale Adversaries （CASA）と共同で、同攻撃を防ぐための暗号技術 SCARF を開発しました。SCARF は、同攻撃への対策の一つであるキャッシュランダム化を現代のコンピュータで安全に運用するために専用に設計されたものであり、数学的解析・定式化によりそのセキュリティが保証されます。この技術は、今後開発されるコンピュータの高セキュリティ化に貢献すると期待されます。

この成果は 2023 年 8 月 9 日から 11 日に米国カリフォルニア州アナハイムで開催される情報セキュリティに関する国際会議 USENIX Security Symposium '23 で発表されます。

【詳細な説明】

研究の背景

パソコン（PC）やスマートフォンなど，現代のコンピュータは非常に高速な処理が可能ですが、データを一時的に格納する主記憶装置（メインメモリ）の処理速度が相対的に遅く、データアクセスの待ち時間が問題となります。そこで、現代のコンピュータは、内部に高速で小規模なメモリ（キャッシュメモリと呼ばれます）を設置し、一度呼び出されたデータを同メモリに格納することで、次回以降そのデータにアクセスするための時間を大きく削減して高い性能を達成しています。一方で、スパイプログラムと呼ばれる悪意あるプログラムを用いて，このキャッシュメモリに残留するデータを悪用して秘密情報（パスワードや暗号鍵など）を外部から不正に取得するキャッシュサイドチャネル攻撃と呼ばれる脆弱性（図 1）が知られており、その対策が急務となっていました。しかしながら、この脆弱性はコンピュータの動作原理に起因していることから、対策技術の開発は困難とされていました。

有望な対策技術の一つとして、キャッシュランダム化が提案されていました。これはキャッシュメモリ内のデータの格納場所をスパイプログラムに分からないようにランダム化（一種の暗号化）する技術です。しかしながら具体的にどのようにランダム化すれば安全なコンピュータが作れるかは不明でした。実際に、これまでいくつかのキャッシュランダム化方式が提案されていますが、その脆弱性もいくつか指摘されています。またランダム化に時間がかかってしまうとコンピュータの性能が低下してしまいます。したがって、現代のコンピュータで運用可能な安全かつ高速なランダム化方法が強く求められていました。

今回の取り組み

東北大学電気通信研究所環境調和型セキュア情報システム研究室の上野嶺助教は、日本電信電話株式会社社会情報研究所およびドイツ・ルール大学ボーフム（RUB）の Cyber Security in the Age of Large-Scale Adversaries （CASA）と共同で、キャッシュサイドチャネル攻撃を防ぐためのキャッシュランダム化暗号技術 SCARF を開発しました（図 2)。今回開発した技術は、これから開発される多くのコンピュータのセキュリティ基盤技術として高安全化に貢献することが期待されています。

本成果では、まずスパイプログラムが実際に実行できることは何なのかを調査・解析し、その能力を数学的に定式化することで、キャッシュランダム化の安全な運用に必要な暗号方式の条件を適切に設定しました。そしてキャッシュランダム化専用の暗号技術 SCARF を具体的に設計しました。SCARF は、キャッシュランダム化に特化することで、安全かつ極めて低遅延にキャッシュランダム化を実現可能です。既存の汎用暗号に比べて、SCARF は約半分の遅延でランダム化を完了します。SCARF の設計には、上述の調査・解析や定式化が最大

限活かされています。

今後の展開

SCARF は暗号技術としての性能評価や、コンピュータに実装した場合のシミュレーションを通して、その高い性能や実用性が検証されています。SCARF は現代の多くのコンピュータに適合するように設計されており、これらに SCARF を適用して安全性・実用性のさらなる検証をすすめます。当該技術を通して、現代情報社会における基盤インフラとも言えるコンピュータの安全性向上に貢献することを目指します。

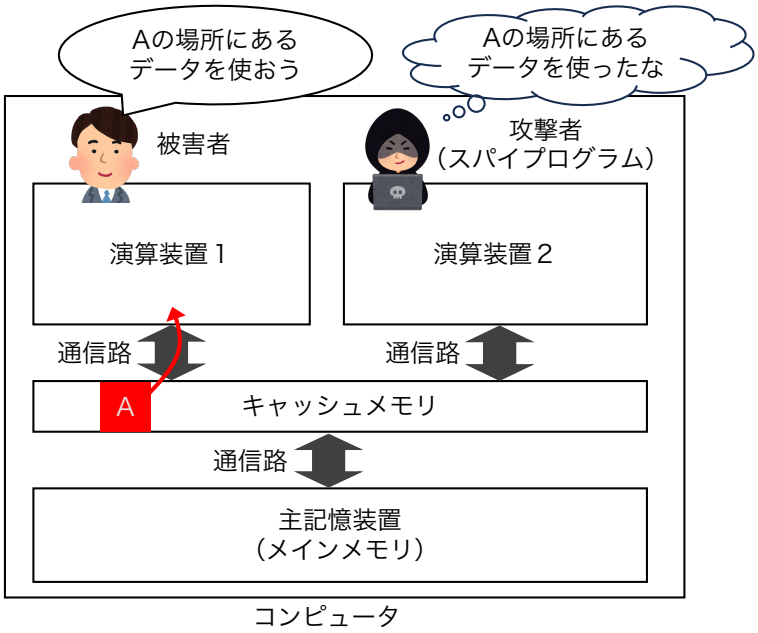

図 1. キャッシュサイドチャネル攻撃の概要。攻撃者はスパイプログラムと呼ばれる特殊なプログラムを用いて被害者がどのデータにアクセスしたかを監視し、それを繰り返すことで秘密のデータを盗み取る。

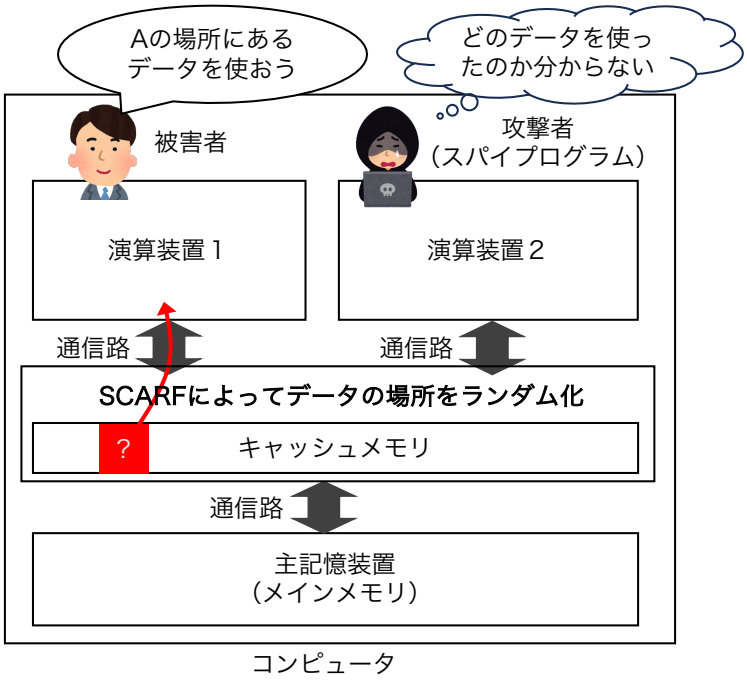

図 2. 開発技術 SCARF を用いたキャッシュランダム化に基づく安全なコンピュータ。攻撃者はスパイプログラムを用いても被害者がどのデータにアクセスしたのか分からない。

【用語説明】

注1.　スパイプログラム：ここでは、メインメモリのどのデータがキャッシュメモリ上にロードされたかを特殊な技法（専門的には、例えば Prime+Probe などと呼ばれる）を用いて推測するプログラムを指す。悪意ある攻撃者はこのスパイプログラムから得られた情報をもとに秘密情報を詐取する。

注2.　サイドチャネル攻撃：正規の入出力以外の副次的な物理情報（処理時間や消費時間）を利用して秘密情報を盗み出す攻撃の総称。キャッシュサイドチャネル攻撃ではデータへのアクセス時間をサイドチャネル情報として利用する。

【論文情報】

タイトル：SCARF: A Low-Latency Block Cipher for Secure Cache-Randomization

著者：Federico Canale, Tim Güneysu, Gregor Leander, Jan Philipp Thoma, Yosuke Todo, and *Rei Ueno

※本学の代表研究者 東北大学 電気通信研究所 助教 上野嶺

掲載誌：Proceedings of The 32rd USENIX Security Symposium

URL: https://eprint.iacr.org/2022/1228

【問い合わせ先】
（研究に関すること）
東北大学電気通信研究所
助教　上野嶺
TEL: 022-217-5507
E-mail: rei.ueno.a8@tohoku.ac.jp

（報道に関すること）
東北大学電気通信研究所　総務係
TEL: 022-217-5420
E-mail: riec-somu@grp.tohoku.ac.jp