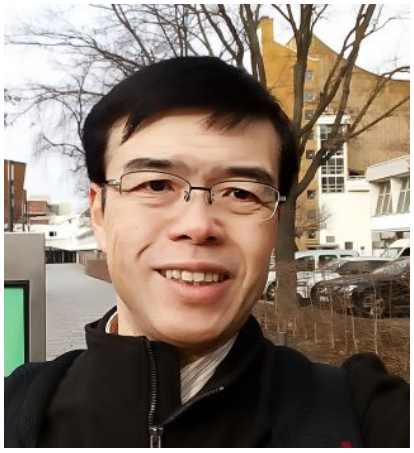
須崎研究室

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

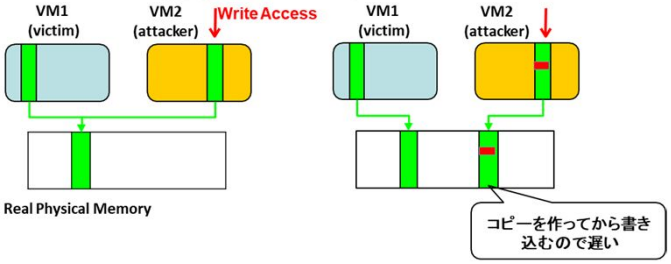
システムソフト(OS, 仮想化など)やハードウェア(TEE, RISC-Vなど)のセキュリティ研究

---クラウドからIoTまで---



クラウドで使われる仮想化の脆弱性(メモリ重複除外)

VMのメモリ節約で使われるメモリ重複除外(Memory Dedeuplication)で書き込みが起こるとアクセス速度が変わることによる脆弱性。他のVMで使われいるソフトウェアや鍵などの類推ができる。

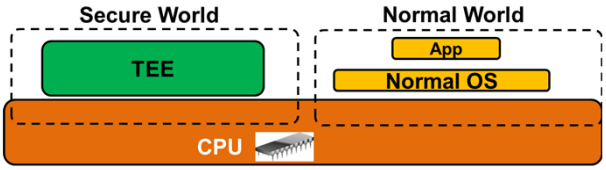


最初の発見者として一流国際会議で紹介

The first memory-deduplication attack, demonstrated by Suzaki et al. [50], was used to detect applications running in other virtual machines. Owens et al. [41] also exploited

TEE(Trusted Execution Environment) 信頼できる実行環境

近年のCPUにはOSとは独立して安全にプログラムを実行でいるTEE(Trusted Execution Environment)がある。携帯ではArmのTrustZoneが使われ、PCではIntel SGXが使われており、これらを活用した研究。



新しいCPUアーキテクチャ RISC-V

IntelやArmなどの商用CPUとは異なり、オープンな命令セットで多くの研究機関で　セキュリティの研究に活用されている。FPGAで実装でき、セキュリティ拡張の研究を行う。

今後のターゲット

- データセンターセキュリティ
- 車載セキュリティ
- ゲームセキュリティ
- デバイス認証
- インシデントトレース
- ペネトレーションテスト
- AIセキュリティ
- Zero-Trust IoT (CREST21-26プロジェクト)

指導教員紹介: 須崎有康(Kuniyasu Suzaki)

東京都青梅市出身。東京農工大学(学士、修士)、東京大学(博士)。
産業技術総合研究所を経て情報セキュリティ大学院大学教授。
IPA未踏2004, 2005。KNOPPIX日本版の作者でIPA日本OSS貢献賞
BlackHat, CODE BLUE, Linux Symposiumで発表。