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
セキュリティ
OS, Virtualization,
Confidential Computing

ハードウェア
セキュリティ
FPGA, RISC-V, TEE,
Open Hardware,
Game Machine

---クラウドからIoTまで---

CPU内蔵FPGAのセキュリティ

CPUを内蔵するFGPAはメモリやデバイスを共有しており、悪意のある攻撃が考えられる。

オープンハードウェア RISC-Vのセキュリティ

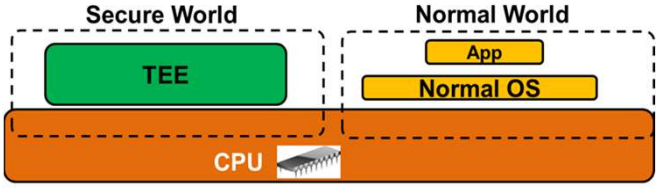
IntelやArmなどの商用CPUとは異なり、オープンハードウェアRISC-V を活用するセキュリティの研究。

船舶システムのセキュリティ

GPSスプーフィングによる船舶の悪意のある誘導やハッキングによる操船制御の乗っ取りなどに対応できるセキュリティの研究。

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がある。携帯ではArmのTrustZone、PCではIntel SGXが使われており、これらを活用した研究。



指導教員紹介: 須崎有康（Kuniyasu Suzaki）
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。