SoC FPGAの主記憶に存在する AES鍵のライブフォレンジック

Live forensics of AES keys in main memory of SoC FPGA

澤 豊文・マネジメント分科会・情報セキュリティ大学院大学

SoC FPGAではCPUとFPGA主記憶を共有することからFPGAを用いたライブメモリフォレンジックが可能。
AESの鍵を対象に暗号ライブラリ・システムソフトウェア・ハードウェアの相互作用によって、開発者が意図しない暗号鍵の複製や消去されずにメモリ上に残り続ける鍵が存在しないか実態を明らかにする。

実績

- CSS2023　デモンストレーションセッション発表
  「アプリの暗号鍵を窃取するSoC FPGAの脅威」
- SCIS2024　口頭発表
  「SoC FPGAの主記憶に存在するAES鍵のライブフォレンジック」

今後

- 作成した回路を使って暗号鍵管理の実態を調査
- 成果をまとめて国際会議に投稿