つくば事業所　共同研究事業について
－取り組みと保有設備の紹介－

産業技術総合研究所　情報セキュリティ研究センター

背景と目的

システムLSIのセキュリティを実現するためには、ベンダーが各々研究開発するだけではなく、我が国として効率的な研究開発投資という視点が重要です。

システムLSIのセキュリティ評価制度および評価体制の確立を我が国が目指す中で、産総研は業界と連携したチップセキュリティ技術の研究開発への貢献を期待されています。

経済産業省の支援により、つくば事業所にチップセキュリティの共同研究施設を整備すると共に、各種評価装置を用いて企業等との共同研究を進めています。

将来に亘る研究開発の戦略を立てるためには、まず、システムLSIに対する攻撃手法と評価手法について、技術トレンドを把握する必要があります。

また、技術を系統的に蓄積する手段の一つとして、確立した評価手法をツールとして整備しようとしています。

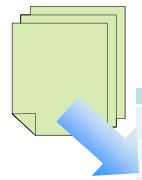
さらに、大学との技術交流を行い、可能な連携の姿を明らかにしつつ、我が国の技術力の結集を目指します。

具体的取り組み

1. 攻撃技術の調査

90年代半ば以降、現在までの学術文献を網羅的に調査するとともに、公開されているCC関連文書を参考に、システムLSIに対する攻撃事例集として整理します。本取組はICSS-JCへの貢献として、ECSEC組合、IPAと共同で進めます。

攻撃手法や技術レベルは時間と共に高度化するため、このような調査を継続してゆくことが大切です。



文献調査

攻撃事例集

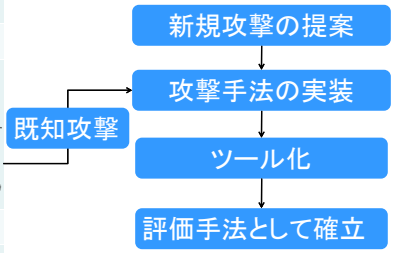
	Author	Title	Conference	Year	重要文献のアブストラクト
1	R. Anderson, M. Kuhn,	Tamper Resistance a Cautionary Note	2nd USENIX Workshop on Electronic Commerce	1996	
2	D. Boneh, R. A. DeMillo and R. J. Lipton	A New Breed of Crypto Attack on "Tamperproof" Tokens Cracks Even the Strongest RSA Code		1996	
3	P.C. Kocher	Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems	CRYPTO '96	1996	秘密鍵を用いた演算に係る処理時間を計測することで、Diffie-Hellman のべき指数やRSA の鍵を求めることができることを示している。秘密鍵の異なる原因としては、不必要な処理のバイパス、条件分岐、RAM キャッシュヒット、処理時間の異なるプロセッサ命令などが挙げられる。べき乗演算に対しては、秘密鍵のビットの値によって処理時間が異なること、中国人剰余定理(CRT)を用いた場合はModular Reduction 処理の有無で処理時間が異なることを利用した攻撃のアイデアが示されている。
4	R. Anderson, M. Kuhn,	Low Cost Attacks on Tamper Resistant Devices	Security Protocols 5th International Workshop	1997	
5	D. Boneh, R. A. DeMillo, R. J. Lipton	On the Importance of Checking Cryptographic Protocols for Faults	Eurocrypt '97	1997	

2. 企業・業界との連携

企業との個別共同研究やECSEC組合との共同研究を通じて、実チップに対する評価技術の研究とツールによる実証を進めます。

攻撃コンセプトは既知であっても、実際にチップにこれを適用し、さらに安全性の評価手法として確立するには、評価手法の実装、ツール化など現実的な課題を解決する必要があります。

また、新たな評価指標となりうる、新しいコンセプトに基づく攻撃の探索も行っています。



3. 大学等との交流・連携

産業界と並行して、大学等もシステムLSIのセキュリティの研究を活発に行っています。

産業界のニーズと学術的な研究ポテンシャルを結び付けることで、双方にメリットが生まれる可能性があります。

連携を進めるには、情報の管理など解決すべき課題もありますが、大きな成果が期待できる分野であり、慎重かつ積極的な取り組みが必要です。

[略号] CC: Common Criteria, ICSS-JC: IC System Security-Japan Consortium, ECSEC: 電子商取り引安全技術研究組合, IPA: 情報処理推進機構

保有設備

化学実験室

ワイヤー＆ダイボンダー

集束イオンビーム装置 (FIB)

エッチング装置
（共有施設）

時間分解エミッション顕微鏡
(TriPHEMOS)

システムLSIに対する脆弱性評価の手法を研究し、実チップで検証するために、ドラフトチャンバーを備えた化学実験室など写真に示す各種装置に加え、レーザー、プローバー、サーモストリーマ等、最新の装置と設備を備えています。

お問い合わせ先

(独)産業技術総合研究所 情報セキュリティ研究センター ICSS技術チーム
http://www.rcis.aist.go.jp/index-ja.html