様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 １０ 日現在

機関番号：２４３０４
研究種目：若手研究
研究期間：2018～2021
課題番号：１８Ｋ１８０５３

研究課題名（和文）RFハードウェアトロイの脅威分析と対策技術の開拓

研究課題名（英文）Threat Analysis and Countermeasure Techniques for Hardware Trojans using Radio-frequency Communication

研究代表者

衣川　昌宏（Kinugawa, Masahiro）

福知山公立大学・情報学部・准教授

研究者番号：００７１０６９１

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究では、電子機器の情報セキュリティの安全性を低下させるハードウェアトロージャン（HT）による回路改変攻撃のうち、攻撃痕跡を残さず遠隔攻撃が可能な意図的電磁妨害（IEMI）をトリガとして動作するHTである無線（RF）HTについて、RFHT攻撃耐性を有する電子機器の基礎的設計手法に関する以下の成果を得た。（1）RFHTとIEMIによる電子機器の情報機密性低下の検証、（2）RFHTが電子回路に挿入される事で生じる電子回路への影響の解析、そして、（3）電子回路へ挿入されたRFHTの検出手法として、電子回路の真正性確認を電子回路自体でセルフチェック可能手法を開発した。

研究成果の学術的意義や社会的意義
電子機器の電子回路は情報セキュリティの信頼性の根源（Root of Trust）であるが、その真正性維持については十分な議論がなされておらず、電子回路への回路改変攻撃が行われた場合、上位レイヤでの情報保護技術による検出は困難であり、その回路上で動作するOSやアプリケーションソフトウェアの信頼性の低下を招く脅威となる。本研究では、攻撃の痕跡が残らない無線を用いたハードウェアトロージャン(RFHT)による電子機器の情報機密性低下について検証を行うと共に、情報セキュリティ、環境電磁工学の2分野の知見を併せ、電子回路レベルでRFHTによる回路の真正性低下を検出可能な基礎的な自己診断技術を開発した。

研究成果の概要（英文）：This research has developed fundamental technologies to guarantee the authenticity of the electric circuits, which are modified with hardware Trojans (HT), which use intentional electromagnetic interferences (IEMI) to trigger HT's malicious function, which leaks information via radio wave. This research calls the HT using IEMI RFHT (radio-frequency HT). The following technologies were developed to achieve the above goals. (1) Verification of decreasing information confidentiality caused by RFHT excited with IEMI. (2) Analysis of changes in electrical parameters of the target electrical circuit when the RFHT is inserted. (3) Self-checking method of the authenticity of the target circuit, which detects RFHT insertions.

研究分野：情報セキュリティ

キーワード：電磁波セキュリティ　ハードウェアトロイ　真正性保証　環境電磁工学　情報セキュリティ

１．研究開始当初の背景

電子機器の信頼性・安全性は、信頼性の高いハードウェアを基礎としてその上にファームウェア、OS、ネットワーク、アプリケーションソフトウェアとレイヤを積み上げることによって、上位層が下位層を信頼することにより機器全体の信頼性・安全性を成り立たせている。しかしながら、そのハードウェアの真正性を脅かす脅威が集積回路（IC）で発見され、それに対する研究が米国国防高等研究計画局(DARPA)による IC の信頼性に関する研究開発を皮切りに 2007 年より開始された。学術分野でも 2007 年より IC 及び情報セキュリティ分野でハードウェアトロージャン（HT: Hardware Trojan）問題として、悪性ハードウェアに関する研究が始まった。

HT 問題は IC 分野で発見されたが、現在では IC だけでなく、集積度が高くなっている IC 周辺のプリント配線基板（PCB: Printed Circuit Board）やケーブルなどの電子機器の構成要素全体がその脅威下にあることが判明している。その IC 周辺要素に対する HT 攻撃対策研究は、環境電磁工学における電磁妨害問題および、電磁ノイズによる情報漏えい問題「電磁的情報漏えい」が出発点である。電子機器は PCB やケーブルなどを有し、電磁波を受信・放射しやすい構造を持っている。そのため、それらに誘起した高周波電流によって HT に攻撃指示もしくは電力供給が可能となっている。また、HT は誘起した高周波電流の変調も可能であり、その信号を再放射することで内部情報を漏えいさせることも明らかとなっている。しかも、その攻撃は電磁波照射時のみ有効化されるため、発見が困難である。この種の HT を本応募では無線 HT（RFHT）と定義する。この RFHT はトランジスタ 1 つで実装可能であり、電子機器への挿入が用意であることから、電子機器に RFHT が挿入されるタイミングは、機器の設計・製造時から機器出荷後の輸送、エンドユーザによる機器の使用中に渡り、機器の廃棄までその脅威は持続する可能性がある。

すなわち上述の検討では「実際の RFHT は電子機器の情報機密性を低下させる脅威であるのか？」という問いを投げかけており、RFHT 挿入による電子機器の回路改変が生じた際に生じるとされる情報機密性低下による情報漏えいが、攻撃者にとって有用な攻撃手段である場合、その電子機器で動作するアプリケーションの情報セキュリティの安全性が低下することを示唆しており、これまでソフトウェア等の上位レイヤで検討されてきた機器の安全性を保つ手法とは異なる電子回路レベルでの対策が求められる。

２．研究の目的

これまで電子機器出荷後に挿入される HT および RFHT による情報セキュリティの安全性低下は十分な議論がなされておらず、意図的電磁妨害（IEMI）を通じて RFHT を遠隔起動することによる情報機密性低下を用いた情報窃盗が行われた場合、上位レイヤにおける情報保護技術による検出は困難であり、電子回路の真正性に依存してきた暗号化されていない平文のデータは直接的にその脅威にさらされ、電子機器全体の機密性低下をもたらす新たな脅威となる。

本研究の目的は、IEMI と RFHT を併用した、危険性の高い情報セキュリティの脅威に対する対策手法の確立である。現在、ハードウェアの改変による情報セキュリティへの攻撃が顕著化している。これまでは、電子機器外部に情報窃盗装置(スキミング等)を接着させる程度であったが、今後はより発見が困難で攻撃成功率が高い確実な手法へと攻撃が進化していくと考えられる。そのため、それに先んじて RFHT と IEMI 併用攻撃の対策を行うことで、技術レベルの低い攻撃も含めて防御・対策手法を確立することを目的とする。

３．研究の方法

本研究では、身の回りに存在するありとあらゆる電子機器、例えばスマートスピーカやパーソナルコンピュータ、ホーム・ビルオートメーション、自動車などに対する RFHT を用いた攻撃による電子機器の真正性低下および情報機密性の低下を防止する基盤技術の開発を行う。

具体的には、（１）IC 周辺部位へ RFHT が挿入（仕掛けられる）される可能性を単純化モデルで検討した後に、電子機器実機に RFHT を挿入し、RFHT が動作し信号情報を漏えいさせるか検証を進めると共に、（２）RFHT が挿入された電子機器に IEMI を照射した際に情報機密性の低下が実際に生じることを、RFHT が反射波として外部へ放射する電磁波より情報の復元を行うことで、情報セキュリティへ与える影響の評価を行う。また、（３）電子機器の電子回路に挿入された RFHT は小型で発見が困難であるため、その電子機器の電子回路に真正性のセルフチェック機能を実現する機構の開発を進める。

４．研究成果

（１）IC 周辺部位に RFHT が挿入される可能性を単純化モデルで検討した後に、電子機器実機を用いて情報機密性の低下の発生に関する基礎的な検討を行った。単純化モデルではターゲットとなる信号配線とアンテナ構造を PCB に作成し、情報漏えいの程度を RFHT からの反射波の電力を指標として評価した。その結果 PCB 上に作成された効率（利得）の低いアンテナであっても、5m程度離れた場所から漏えい情報の復元か可能であることが判

明した。情報機器実機に対しては、情報機器本体に内蔵された PCB にアンテナ構造をカッターナイフ等で加工するだけで、容易に RFHT が動作する環境を構築できることが分かった。

（2）IEMI を RFHT に照射した際に生じる、RFHT とアンテナ構造からの反射波から情報の復元を行い、情報漏えいの程度について検討を行った。その結果ディジタル信号およびある程度周波数の高い（約 100 kHz～）アナログ信号であれば、信号の復元が可能であり、情報窃盗が生じる可能性があることを示した。実際の通信プロトコルでは、USB Full/Low-Speed や PS/2 キーボードの通信線、スマートスピーカの PDM マイク信号等のディジタル信号、アナログ RGB 信号や暗号処理ボードの電源-グラウンド間に生じるサイドチャネル信号等のアナログ信号等の幅広い機器がターゲットになることを示した。

（3）電子機器に RFHT が挿入されても電子機器自体の動作に影響を及ぼさず、また機器を開封して RFHT の挿入を視覚的に検査するのも、その小型さから発見は困難である。また RFHT が挿入されるタイミングは機器の設計・製造だけでなく、機器がエンドユーザに使用されている期間も含む。そのため電子機器のライフタイムにおける電子回路のセルフチェック機能が必要とされる。その電子回路の真正性確認の手法は、従来では計測器を用いて RFHT の挿入を診断する必要があり、エンドユーザが機器を使用している期間では機器の使用を中止する必要があり、実行が困難であった。そこで本研究では RFHT が挿入されることで、回路の静電容量が変化することに着目し、機器の PCB 上に実装されているマイクロコントローラの静電容量式タッチセンサ機能を RFHT の挿入検出に使用する事で、電子機器に計測用の電子部品を追加することなく、セルフチェック機能を実現した。

本プロジェクトの成果（1）～（3）は、IEEE EMC Society International Symposium on EMC+SIPI 及び The Asia-Pacific International Symposium on Electromagnetic Compatibility のスペシャルセッションにて招待講演を行った。

また暗号ハードウェア・ハードウェアセキュリティの国際会議 Cryptographic Hardware and Embedded Systems で口頭発表し、IACR Transactions on Cryptographic Hardware and Embedded Systems にて論文発表を行った。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Masahiro Kinugawa, Daisuke Fujimoto, Yuichi Hayashi	４．巻 2019
２．論文標題 Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure	５．発行年 2019年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)	６．最初と最後の頁 62-90
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tches.v2019.i4.62-90	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

〔学会発表〕　計7件（うち招待講演　3件／うち国際学会　3件）

１．発表者名 Masahiro Kinugawa, Yuichi Hayashi
２．発表標題 Board-Level Hardware Trojan Detection Using Sensing Function of on-Board ICs in IT Devices
３．学会等名 2021 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2021)（招待講演）（国際学会）
４．発表年 2021年

１．発表者名 Masahiro Kinugawa, Yuichi Hayashi
２．発表標題 Possibility of Injecting Malicious Instructions from Legitimate Communication Channels by IEMI
３．学会等名 2020 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI)（招待講演）（国際学会）
４．発表年 2020年

１．発表者名 Masahiro Kinugawa, Yuichi Hayashi
２．発表標題 A Study on Feasibility of Electromagnetic Information Leakage Caused Forcibly by Low-Power IEMI
３．学会等名 2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)（招待講演）（国際学会）
４．発表年 2019年

１．発表者名
西鳥羽陽，衣川昌宏

２．発表標題
電磁照射による意図的な情報漏えい誘発時の上限周波数に関する基礎検討

３．学会等名
2019年度電気関係学会東北支部連合大会

４．発表年
2019年

１．発表者名
川上莉穂，鍛治秀伍，衣川昌宏，藤本大介，林優一

２．発表標題
電磁照射による意図的な情報漏えい誘発時に生ずる自己干渉波の抑制に関する基礎検討

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
S. Wakabayashi, S. Maruyama, T. Mori, S. Goto, M. Kinugawa and Y. hayashi

２．発表標題
A Feasibility Study of Radio-frequency Retroreflector Attack

３．学会等名
12th USENIX Workshop on Offensive Technologies (WOOT '18)

４．発表年
2018年

１．発表者名
硲マーティン，衣川昌宏，藤本大介，林優一

２．発表標題
意図的な電磁波注入による漏えい情報の制御に関する基礎検討

３．学会等名
電子情報通信学会 ソサイエティ大会

４．発表年
2018年

〔図書〕　計1件

１．著者名 林優一，衣川昌宏	４．発行年 2021年
２．出版社 科学技術出版	５．総ページ数 10
３．書名 月刊EMC「電磁的セキュリティと情報通信機器の信頼性確保 ハードウェアトロイによる情報漏えいの脅威」	

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関