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　　元 年　　６ 月 １２ 日現在

機関番号：１４６０３
研究種目：基盤研究(B)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０２８３１

研究課題名（和文）公共空間におけるスマートデバイスに対する物理攻撃への対策スイートの研究開発

研究課題名（英文）Development of Countermeasures against Remote Visualization of Screen Images Using EM Emanation from Smart Devices in Public Space

研究代表者
林　優一（Hayashi, Yuichi）

奈良先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：６０５５１９１８

交付決定額（研究期間全体）：（直接経費）　　13,200,000円

研究成果の概要（和文）：本研究は、公共空間におけるスマートデバイスからの電磁波による情報漏えい評価技術の開発・メカニズム解明・対策技術の開発に取り組んだ。具体的には、漏えい評価技術を開発し、その評価技術を用いて、デバイスから生ずる漏えい電磁界を時間領域で可視化することにより、漏えいメカニズムを解明した。また、メカニズムに基づき、漏えいに関わる設計パターンを特定し、そのパターンに着目した情報漏えいを予測可能なシミュレーション技術を開発した。さらに、メカニズムに基づき、漏えいを抑止する配線パターンや電気素子などを効果的に組み合わせ、安価で機器に実装しやすい対策技術を開発した。

研究成果の学術的意義や社会的意義
タブレット端末は近年急激に普及しており、私的な空間のみならず第3者が存在する公共の空間においても個人的な情報を閲覧・入力する機会が増加している。一方で、タッチスクリーン端末に表示された情報が電磁波を通じて漏えいする新たな脅威が指摘されており、攻撃の痕跡を残さずにユーザが端末に入力したキーとその入力先が攻撃者に漏えいする可能性がある。本研究ではこうした脅威に対抗するため電磁波を通じた漏えい評価技術及びメカニズムを解明し、それに基づく対策技術の開発を行った。

研究成果の概要（英文）：In this research, we developed evaluation and simulation techniques and countermeasures against electromagnetic (EM) information leakage from smart devices in public spaces. We also investigated the mechanism of EM information leakage. Specifically, we developed leak evaluation methods and used these to visualize the leaked EM field emitted from the target device. Then, based on the results, we clarified the leakage mechanism. Moreover, based on this mechanism, we identified design patterns on PCB boards related to such leakage and developed predictive simulation techniques. Furthermore, based on the identified mechanism, we have effectively combined the associated wiring patterns and electrical elements to prevent leakage, thereby developing inexpensive countermeasures that can be easily installed onto the target equipment.

研究分野：情報セキュリティ、環境電磁工学

キーワード：電磁情報セキュリティ　サイドチャネル攻撃　スマートデバイス　電磁環境　ディスプレイ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

タッチスクリーンを搭載したスマートホン、タブレットなどのスマートデバイスの急激な普及に伴い、その利便性から私的な空間のみならず第 3 者が存在する公共の空間においても個人的な情報を閲覧・入力する機会が増加している。一方で、タッチスクリーン型の端末は、従来の PC などと異なり、スクリーン上に表示されるソフトウェアキーボードで入力操作を行うため、入力したキーとその入力先が同一画面に表示される。そのため、画面を盗み見されるとそれらの情報が同時に知られてしまうことになる。特にソフトウェアキーボードでは、ユーザに通知する目的で押下したキーを色の反転やポップアップにより強調表示するため、パスワード入力時などの入力した文字が伏せ字になる場合でも、タッチしたキーの情報とその入力先の情報から、何をどこに入力したのかを判別できる。さらに、こうした情報が電磁波を通じて漏えいした場合には、盗視の痕跡を残さずに情報を取得できる可能性があり、重大なセキュリティリスクをもたらす可能性がある。しかし、デバイス自体の消費電力が小さいことから、情報を含んだ放射電磁界強度も相対的に弱く、さらに、移動しながら利用されることが多いことから、電磁波を介した盗み見（電磁的画面盗視）の対象としては見なされず、その危険性に関する十分な検討はなされていなかった。

これに対し、本研究代表者のグループはプロファイリングや信号処理技術を用いることにより、可搬性のある装置による電磁的画面盗視の脅威がタブレット端末に存在することを明らかにした。これまでの電磁的画面盗視では主に、据え置き型のディスプレイが対象とされ、盗視のための装置は一般に大がかりとなり、屋内や車内に設置されて使用されることが想定されてきたため、ディスプレイから漏えいする電磁波が装置に到達する前に、信号レベルを背景雑音以下に減衰させることで盗み見を防止するゾーニングという概念の下に対策がとられてきた。しかし、本研究代表者が明らかにした新たな脅威は、これまでの前提条件を覆すものであり、従来の電磁的画面盗視とは異なる対策が求められる。

２．研究の目的

本研究では、スマートホンやタブレットなどのスマートデバイスにおける電磁情報漏えい評価及び対策技術の確立を目指し、情報漏えい評価法から対策技術の開発まで次の 4 項目を目的とする。(1)スマートデバイスからの漏えい評価技術の開発、(2)評価技術に基づいたスマートデバイスからの情報漏えいメカニズムの解明、(3)電磁界シミュレーション技術を用いた機器設計情報に基づく漏えい評価技術の開発、(4)漏えいメカニズムに基づいた安価で機器に実装しやすい対策技術の開発

３．研究の方法

上述した各目的を達成するために行った研究方法は以下の通りである。

(1)スマートデバイスからの漏えい評価技術の開発

これまで開発した漏えい電磁波評価環境を拡張し、多種多様なスマートデバイスからの漏えい評価を可能にするシステムを構築した。具体的には、画面描画に応じて生ずる漏えい電磁波は振幅変調され周期を持つことを利用し、「複雑な画面再構築処理を必要としない信号復調」と「モデルを用いた周期の自動検出」を行うことで漏えいの有無を高速に判定できる評価技術を開発した。

(2)評価技術に基づいたスマートデバイスからの情報漏えいメカニズムの解明

上記で開発を行った評価システムによって、電磁波を通じた情報漏えいが確認されたスマートデバイス内外の電磁界伝搬を高時間・高空間分解能で計測した。計測された電磁界を時系列で可視化することにより、漏えいメカニズムを解明した。

(3)電磁界シミュレーション技術を用いた機器設計情報に基づく漏えい評価技術の開発

上記で解明したメカニズムに基づき、漏えいに深く関わる配線パターン、素子、信号パターンなどを特定し、設計情報からそれらの構造を抽出し、設計段階で漏えいを予測可能なシミュレーションモデルを構築した。

(4)漏えいメカニズムに基づいた安価で機器に実装しやすい対策技術の開発

上記で明らかにしたメカニズムを基に、配線パターンなどの幾何的な形状及び、環境電磁工学分野で開発されたノイズ抑制素子、これまでに開発した電磁界センサなどを効果的に組み合わせ、スマートデバイスに適用可能な対策技術を開発した。

４．研究成果

研究成果として、端末から画面描画情報が漏えいするモデル（これを以後「漏えいモデル」と呼ぶ）を構築し、そのモデルに基づき情報を漏えいさせる周波数（これを以後「漏えいチャネル」と呼ぶ）を高速に推定する手法を確立し、デバイスからの漏えいの有無を判定できる技術を開発した。また、機器内部で処理される情報を制御することでより、高速に漏えいの有無を判定できる技術も開発した。さらに、上述の評価法を用いることで情報の漏えいは画面描画に関わるデータをシリアルに処理する IC 及びケーブルを漏えい源とし、それらの信号が伝送される際、屈曲部などを有する部分から寄生結合を通じて周囲の導体に信号が漏えいすることにより生ずることを明らかにした。

前述のメカニズムにより、情報を含む電磁放射は機器を構成する基板のサイズや信号を伝送

するケーブル長などの物理構造により引き起こされると予想されることから、設計データからこうした物理構造のみを抽出した簡易的なシミュレーションモデルを構築した。さらに、メカニズムを基に漏えい源から攻撃者が所有する受信アンテナまでの伝搬経路上の漏えい電磁波レベルを大幅に低減することで、漏えい電磁波を通じた情報取得の脅威に対抗する手法を開発した。伝搬経路には漏えい源からアンテナまで電磁信号を誘導するカップリングパス、機器を構成するプリント基板上の配線パターンや接続線路など機器の幾何的構造により構成されるアンテナ及び、電磁波が放射されてから受信されるまでの空間が含まれるため、これらに対し、漏えい源近傍にデカップリング回路を形成する手法や機器の筐体やケーブルから漏えいを抑制する電磁シールド手法などを適用し、これまで開発を行ったシミュレーション技術を用いて評価を行いながら、スマートデバイスに適用可能な対策技術の開発を行った。

これまで検討を行ってきた漏えい電磁波によるセキュリティ低下の脅威に関して、電磁波の伝搬を逆向きに考えることで、これまで得られた知見を妨害電磁波によるセキュリティ低下の脅威にも応用できる可能性についても基礎的な実験を通じて明らかにした。

５．主な発表論文等

〔雑誌論文〕（計１２件）

[1] Y. Hayashi, N. Homma, “Introduction to Electromagnetic Information Security,” IEICE Transactions on Communications, Vol.E102-B, vol.1, pp.40-50, 2019. https://doi.org/10.1587/transcom.2018EBI0001.（査読有り）

[2] V. Yli-Mayry, D. Miyata, N. Homma, Y. Hayashi and T. Aoki, "Statistical Test Methodology for Evaluating Electromagnetic Information Leakage From Mobile Touchscreen Devices," in IEEE Transactions on Electromagnetic Compatibility, vol.99, pp.1-8, DOI: 10.1109/TEMC.2018.2866553, 2019.（査読有り）

[3] S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Data Injection Attack Against Electronic Devices With Locally Weakened Immunity Using a Hardware Trojan," IEEE Transactions on Electromagnetic Compatibility, vol.99, pp.1-7, DOI: 10.1109/TEMC.2018.2849105, 2018.（査読有り）

[4] S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, Arthur Beckers, Joseph Balasch, Benedikt Gierlichs and Ingrid Verbauwhede, "EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage," IEEE Transactions on Electromagnetic Compatibility, vol.99, pp.1-7, DOI: 10.1109/TEMC.2018.2844027, 2018.（査読有り）

[5] 藤本大介, 林優一,“実環境で動的構成可能なデジタル回路を用いた IC 内部に伝導するノイズの測定法,”電気学会論文誌 A, vol.138, no.6, pp.335-340, 2018.（査読有り）

[6] 中村 紘, 林優一,“タイミング違反の検出に基づく IC 内部の処理に過渡電磁界の与える影響評価,”電気学会論文誌 A, vol.138, no.6, pp.302-308, 2018.（査読有り）

[7] K. Nakamura, Y. Hayashi, T. Mizuki, and H. Sone, “Information leakage threats for cryptographic devices using IEMI and EM emission,” IEEE Transactions on Electromagnetic Compatibility, vol. 60, no. 5, pp. 1340-1347, 2018.（査読有り）

[8] Y. Hayashi, Jong-Gwan Yook, W. A. Radasky, "Hardware Security for Information/Communication Devices," 2017 Asia-Pacific International Symposium on Electromagnetic Compatibility, p.92, 2017.（査読有り）

[9] 衣川昌宏, 林優一, 森達哉,“意図的な電磁妨害時にハードウェアトロイによって引き起こされる情報漏えい評価,” 電気学会論文誌 A, vol. 137, no.3, pp.153-157, 2017.（査読有り）

[10] Y. Hayashi, N. Homma, Y. Toriumi, K. Takaya, and T. Aoki, “Remote Visualization of Screen Images Using a Pseudo-Antenna that Blends into the Mobile Environment,” IEEE Transactions on Electromagnetic Compatibility, vol. 59(1), pp. 24-33, DOI: 10.1109/TEMC.2016.2594237, 2017.（査読有り）

[11] Y. Hayashi and J.-G. Yook, “Introduction to a Special Session on EMC and Information Security,” In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC’16), pp. 1275-1276, 2016.（査読有り）

[12] Y. Hayashi, W. A. Radasky, “Introduction to EM Information Leakage from Commercial Devices and Its Countermeasure, 2016 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC2016), PID4128815, 2016.（査読有り）

〔学会発表〕（計３３件）

[1] 林優一,“漏えい・妨害電磁波によるセキュリティ低下の脅威と対策," IEEE SSCS Kansai Chapter Technical Seminar, 2018.

[2] 林優一,“情報機器に求められる電磁波セキュリティ," 第４回 極限環境電磁波センシング研究施設ワークショップ, 2018.

[3] Daisuke FUJIMOTO, Takashi Narimatsu, Yu-ichi HAYASHI, "Fundamental Study on the Effect of Torque Value at Connector on Equivalent Circuit of Contact Boundary," 国際セッション IS-EMD2018, EMD2018-47, 2018.
[4] 林優一,“情報セキュリティと EMC," 第 19 回 EMC シンポジウム IIDA2018, シルクホテル, 長野県飯田市, 2018.
[5] 林優一,“電磁波による情報漏えいの脅威とその対策," 奈良先端科学技術大学院大学公開講座 2018, 奈良先端大, 奈良県生駒市, 2018.
[6] 林優一,“IoT 時代に求められるハードウェアセキュリティ," EMC 関西 2018, メルパルク京都, 京都府京都市, 2018.
[7] 硲マーティン, 衣川昌宏, 藤本大介, 林優一, “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,” 2018 年電子情報通信学会ソサイエティ大会, A-20-6, 2018.
[8] Y.Hayashi,“EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan," AMEREM, University of California, Santa Barbara, 2018.
[9] 林優一,“IoT 時代の電磁波セキュリティ～痕跡を残さない攻撃とその対策～," IoT セキュリティフォーラム 2018, よみうり大手町ホール, 東京都, 2018.
[10] Y.Hayashi,“EMC from hardware security perspective," The 1st Croatia-Japan EMC Workshop, University of Zagreb, Croatia, 2018.
[11] 仁科泉美, 藤本大介, 衣川昌宏, 林優一, “スマートデバイスからの電磁情報漏えい源特定に関する基礎検討,” ハードウェアセキュリティ研究会, HWS2018-18, 2018.
[12] 岡本拓実, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, “ガウス雑音を用いた暗号機器への意図的な電磁妨害に対する耐性評価手法,” ハードウェアセキュリティ研究会, HWS2018-17, 2018.
[13] 林優一,“融合領域における EMC 分野の役割と人材育成," 次世代の EMC 研究者・技術者を交えたワークショップ, NICT/EMC-net 将来課題研究会, 情報通信研究機構本部, 東京都小金井市, 2018.
[14] R. Birukawa, G. Tanabe, Y. Hayashi, T. Mizuki, and H. Sone, “A Study on an Evaluation Method for EM Information Leakage Utilizing Controlled Image Displaying,” 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), 2018.
[15] S. Kaji, M. Kinugawa, D. Fujimoto, and Y. Hayashi, "Data Injection Attacks Using a Hardware Trojan on a Transmission Line," 2018 Joint IEEE EMC & APEMC, TU-PM-I-TC-05-3, 2018.
[16] S. Osuka, D. Fujimoto, Y. Hayashi, N. Homma, Arthur Beckers, Joseph Balasch, Benedikt Gierlichs and Ingrid Verbauwhede, "Fundamental Study on Non-invasive Frequency Injection Attack against RO-based TRNG," 2018 Joint IEEE EMC & APEMC, TU-PM-I-TC-05-1, 2018.
[17] 杉本藍莉, 林優一, 水木敬明, 曽根秀昭, 暗号機器からの電磁情報漏えいにおける周波数特性に関する研究, EMC 仙台ゼミナール・IEEE EMC-S Sendai-Ch 学生発表会, no.5, 東北大学サイバーサイエンスセンター, 2018.
[18] 田辺弦太郎, 林優一, 水木敬明, 曽根秀昭, 描画情報の選択を用いた電磁情報漏えいの評価に関する研究, EMC 仙台ゼミナール・IEEE EMC-S Sendai-Ch 学生発表会, no.4, 東北大学サイバーサイエンスセンター, 2018.
[19] 鍛治秀伍, 衣川昌宏, 藤本大介, 林優一, "HT を用いて局所的にイミュニティを低下させた電子機器へのデータ注入攻撃," 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 1D2-3, 2018.
[20] 林優一,“漏えい・妨害・改変の 3 つの視点からみた電磁情報セキュリティ," IEEE EMC Society Sendai Chapter Colloquium, 東北大学, 2017.
[21] 田辺弦太郎, 林優一, 水木敬明, 曽根秀昭, 描画情報の制御時における放射電磁波の特徴量に着目した情報漏えい評価, IEEE Instrumentation & Measurement Society Japan Chapter 2017 年度 第 2 回学生研究発表会, IEEE_IM-S17-30, 東北大学工学部青葉記念会館, 2017.
[22] 杉本藍莉, 藤本大介, 林 優一, 水木敬明, 曽根秀昭, ”周波数選択による暗号機器の情報漏えい評価の効率化に関する検討” 電子情報通信学会信学技報 IEICE Technical Report, EMCJ2017-75(2017-11) pp63-66, 2017.
[23] 田辺弦太郎, 林 優一, 水木敬明, 曽根秀昭, ”表示画像の選択を用いた電磁情報漏えい評価手法に関する検討” 電子情報通信学会信学技報 IEICE Technical Report, EMCJ2017-74(2017-11), pp.57-62, 2017.
[24] Y. Hayashi "EM Information Security Threats and Its Countermeasures," EMC Beijing 2017, China National Convention Center, 2017.
[25] 鈴木 太陽, 林 優一, 石上 忍, 川又 憲, 嶺岸 茂樹, “TEM セルを用いた暗号モジュールへの故障注入攻撃の定量的耐性評価に関する研究," 電気関係学会東北支部連合大会講演論文集, 2017, 2017 巻, 平成 29 年度　電気関係学会東北支部連合大会　講演論文集, セッション ID 2E12, p. 204, 2017.

[26] 林優一,“次世代ワイヤレス通信に求められるハードウェアセキュリティ,” 次世代ワイヤレス技術講座 - KEC 関西電子工業振興センター，ハービス PLAZA，2017.
[27] 林優一,“サイバー空間における攻撃モデルはハードウェアへの物理攻撃にも適用可能か？,”電子情報通信学会総合大会，AS-3-9，2017.
[28] ヴィッレウリマウル，本間尚文，林優一，鳥海陽平，伊丹　豪，鈴木康直，中村雅之，高谷和宏，青木孝文,“ t 検定による電磁的画面情報漏えいの安全性評価手法,”電子情報通信学会総合大会，AS-3-11，2017.
[29] 林優一,“ブルートフォース的漏えいパラメタ推定に基づくモバイル端末への 電磁的盗視の脅威に関する検討,” 電気学会研究会資料，EMC-17-008，pp. 37-39，2017.
[30] 林優一,“電磁波を通じた情報漏えいの脅威とその対策,” 情報セキュリティ研究会・技術と社会・倫理研究会，ライフインテリジェンスとオフィス情報システム研究会，福井市地域交流プラザ，2016.
[31] Y. Hayashi, "EM Information Leakage Threats in Public Spaces," Workshops and Tutorials, IEEE International Symposium on Electromagnetic Compatibility 2016, Ottawa, 2016.
[32] Y. Hayashi, "EM Information Security of Tablet PCs in Public Space," EMC Joint Workshop Taipei, 2016.
[33] 伊丹豪，鳥海陽平，中村雅之，鈴木康直，高谷和宏，林優一，本間尚文，青木孝文,“モバイル端末からの漏えい電磁波を介した画面再現リスク評価手法の検討,”2016 年電子情報通信学会ソサイエティ大会，B-4-52，p. 1，2016.

〔図書〕（計２件）
[1] IoT 時代の電磁波セキュリティ ～21 世紀の社会インフラを電磁波攻撃から守るには～,一般社団法人　電気学会　電気システムセキュリティ特別技術委員会 スマートグリッドにおける電磁的セキュリティ特別調査専門委員会，科学情報出版，分担執筆，林優一，pp.302-309，2017.
[2] IoT 時代のモバイル端末に求められるハードウェアセキュリティ,科学情報出版，分担執筆，林優一，pp. 61-69，2016.

６．研究組織

(1)研究分担者

研究分担者氏名：本間 尚文

ローマ字氏名： Homma, Naofumi

所属研究機関名：東北大学

部局名：電気通信研究所

職名：教授

研究者番号（8 桁）：00343062

研究分担者氏名：嶺岸 茂樹

ローマ字氏名：Minegishi, Shigeki

所属研究機関名：東北学院大学

部局名：工学部

職名：教授

研究者番号（8 桁）：70146116

研究分担者氏名：藤本 大介

ローマ字氏名：Fujimoto, Daisuke

所属研究機関名：奈良先端科学技術大学院大学

部局名：先端科学技術研究科

職名：助教

研究者番号（8 桁）：60732336

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。