論 文 内 容 の 要 旨

博士論文題目

意図的電磁妨害が引き起こす情報セキュリティ低下に関する研究

Information Security Degradation due to Intentional Electromagnetic Interference

氏　名　　西山 輝

（論文内容の要旨）

電子機器への意図的な電磁妨害(IEMI)は、機器内部の回路素子を破壊することで機器の機能を停止させる脅威として知られており、電磁波に対する電子機器の耐性の許容値を遙かに上回る高電力電磁波(HPEM)を手段とする。

従来、HPEM を用いた IEMI による脅威は軍事などの、一部の分野に限られていたが、近年は小型の大電力送信装置などが報告されており、商用製品として広く用いられている電子機器への IEMI の脅威が現実のものとなっており、機器機能が停止するメカニズムや脅威に対する対策が検討されてきた。

これに対し、本論文では HPEM と比べ 3 桁ほど小さいレベルである数 V 程度の電磁妨害波をタイミング制御して印加することにより、機器の動作は保ちつつ、一部の処理やデータのみに意図的に誤りを生じさせ、僅かな機能低下を引き起こし、セキュリティを損なう新たな脅威を検討した。

電子機器内で扱われるデータ信号や制御信号は電流/電圧の時間変化として捉えることができることから、(1)機器内部のデータ信号に対する脅威として、集積回路(IC)を相互接続する伝送路上のデータ信号を対象とし、IEMI により時間および振幅的な擾乱を与えることでデータ信号に誤りが生ずることを示し、完全性が低下することを明らかにした。次に、(2)制御信号に対する脅威として、機器のタイミング制御を担うクロックを対象とし、暗号 IC に供給されるクロックに時間的および振幅的な擾乱を与えることで、暗号 IC 内部の秘密鍵を取得可能であることを示し、機密性が低下することを明らかにした。そして、(3)電気信号に対する擾乱を抑制する機構を備えた機器に対する脅威として、クロックの時間的擾乱を抑制する位相同期回路に着目し、その抑制プロセスを考慮して妨害波を印加することで、抑制機能を無効化できることを示し、機密性および可用性が低下することを明らかにした。

上記を通じて、本論文では、セキュリティの 3 要素である機密性、可用性、完全性を低下させる IEMI の脅威を示した。そして、上述の脅威によるセキュリティ低下のメカニズムを解明し、そのメカニズムに基づいて、電気レベル・回路レベルにおける妨害電磁波抑制技術を組み合わせることにより、上位のアルゴリズムやプロトコルによらない対策技術を実現できることを示した。

氏　名	西山　輝

（論文審査結果の要旨）

本論文では、数 V 程度の電磁妨害波をタイミング制御して電子機器に印加することにより、機器の動作は保ちつつ、一部の処理やデータのみに意図的に誤りを生じさせ、僅かな機能低下を引き起こし、セキュリティを低下させる新たな脅威を示した。さらに、脅威のターゲットとなる機器内で扱われるデータ信号や制御信号を電流/電圧の時間変化として統一的な視点から捉えることで、セキュリティ低下のメカニズムを明らかにした。

本論文の主な成果は以下に要約される。

1. データ信号に対する脅威として、集積回路(IC)を相互接続する伝送路を対象とし、妨害波の印加により時間および振幅的な擾乱を与えることでデータ信号に誤りが生ずることを示し、完全性が低下することを示すと共にそのメカニズムを明らかにした。

2. 制御信号に対する脅威として、機器のタイミング制御を担うクロックを対象とし、暗号 IC に供給されるクロックに時間的および振幅的な擾乱を与えることで、暗号 IC 内部の秘密鍵を取得可能であることを示し、機密性が低下することを示すと共にそのメカニズムを明らかにした。

3. 電気信号に対する擾乱を抑制する機構を備えた機器に対する脅威として、クロックの時間的擾乱を抑制する位相同期回路に着目し、その抑制プロセスを考慮して妨害波を印加することで、抑制機能を無効化できることを示し、機密性および可用性が低下することを示すと共にそのメカニズムを明らかにした。

以上のように、本論文は環境電磁工学と情報セキュリティの知見を融合させ、妨害電磁波の印加によるセキュリティ低下のメカニズムを解明すると共に、そのメカニズムに基づく、電気レベル・回路レベルにおける妨害電磁波抑制技術を組み合わせることで、上位のアルゴリズムやプロトコルによらない対策技術を提案しており、その学術的インパクトは少なくない。よって本論文は、博士（工学）の学位論文としての価値があるものと認める。