電波再帰反射攻撃の実用性評価

若林 哲宇[1,a)]　丸山 誠太[1]　星野 遼[1]　森 達哉[1]　後藤 滋樹[1]　衣川 昌宏[2]　林 優一[3]

概要：電波再帰反射攻撃（RFRA: Radio-frequency retroreflector attack）はアクティブな電磁波漏えいによるサイドチャネル攻撃の一種である．ターゲットに対して電波を照射し，その反射波を解析することでターゲット内を流れる信号を盗聴する．ターゲットには予め仕掛けを施しておく必要があり，仕掛けがされたターゲットをハードウェアトロイと呼ぶ．．仕掛けはターゲットのケーブルに FET のチップを埋め込み，ケーブルのシールド線はダイポールアンテナとして利用する．アンテナは照射した電波を受信し，それをターゲット信号により AM 変調し反射波として放出させる．攻撃者は反射波を AM 復調することでターゲット信号を得ることができる．ハードウェアトロイは FET チップを取り付けるだけで完成し，また FET チップはとても小さいためあらゆるデバイスが攻撃の対象になりうる．例えばキーボードやディスプレイ，スピーカー，マイク，USB を利用して接続されたデバイスなどが挙げられる．これまで RFRA はいくつかの攻撃成功例が報告されてきたものの，実験による攻撃の条件，限界などの調査は少なく攻撃の脅威は不明な部分が多い．本研究では RFRA の限界を調査することで実世界においてどの程度有効であるのかを明らかにした．実験はターゲットまでの距離とターゲット信号の周波数の 2 つの観点から行った．実験装置はすべて市販の装置を利用し，総額も 50 万円程度と誰もが攻撃を行えるという条件のもと（1）最大で 10 Mbps の信号に対する攻撃（2）最大で 10 m の距離からの攻撃に成功した．これらは RFRA が実世界において脅威であることを示すには十分な結果である．

キーワード：システム，電波再帰反射攻撃

Understanding the Feasbility of RF Retroreflector Attack

Satohiro Wakabayashi[1,a)]　Seita Maruyama[1]　Haruka Hoshino[1]　Tatsuya Mori[1]
Shigeki Goto[1]　Masahiro Kinugawa[2]　Yuichi Hayashi[3]

Abstract: Radio-frequency (RF) retroreflector attack (RFRA) is an *active* electromagnetic side-channel attack that aims to leak the target's internal signals by irradiating the targeted device with a radio wave, where an attacker has embedded a malicious circuit (RF retroreflector) in the device in advance. As the retroreflector consists of small and cheap electrical elements such as a field-effect transistor (FET) chip and a wire that can work as a dipole antenna, the reflector can be embedded into various kinds of electric devices that carry unencrypted, sensitive information; e.g., keyboard, display monitor, microphone, speaker, USB, and so on. Only a few studies have addressed the basic mechanism of RFRA and demonstrated the success of the attack. The conditions for a successful attack have not been adequately explored before, and therefore, assessing the feasibility of the attack remains an open issue. In the present study, we aim to investigate empirically the conditions for a successful RFRA through field experiments. Understanding attack limitations should help to develop effective countermeasures against it. In particular, with regard to the conditions for a successful attack, we studied the distance between the attacker and the target, and the target signal frequencies. Through the extensive experiments using off-the-shelf hardware including software-defined radio (SDR) equipment, we revealed that the required conditions for a successful attack are (1) up to a 10-Mbps of target signal and (2) up to a distance of 10 meters. These results demonstrate the importance of the RFRA threat in the real world.

Keywords: System, RF Retroreector Attack

1. はじめに

ハードウェアトロイとはターゲットとなるデバイスに埋め込まれた悪意のある動作をする回路の総称である．ハードウェアトロイの動作としてはターゲットの破壊や，情報を漏えいなどがある．ハードウェアトロイはデバイスの製造者や使用者の意図しないところで仕掛けられるため，その存在に気づきにくい．ハードウェアトロイが埋め込まれるシナリオとしては悪意のあるデバイス製造者が設計時に埋め込むケース，あるいは製造の外注先が秘密裏に埋め込むケースが考えられる．あるいは流通経路に何らかの方法で介入し，完成品に改造を施した製品を流通させるケースも考えうる．

電波再帰反射攻撃（RFRA: Radio-frequency Retroreflector Attack）はターゲットにハードウェアトロイを埋め込むことによって外部からターゲット内部の信号を秘密裏に復元する攻撃である．埋め込むハードウェアトロイはシンプルかつ小型な回路であるため，多くのデバイスがターゲットになりうる．RFRA のターゲットとして最も単純なものはデバイス同士を物理的に接続するケーブルである．埋め込む回路を構成する素子は FET とアンテナとして動作する導線であるが，埋め込むターゲットがケーブルの場合はケーブル内の外部導体 (シールド線) をアンテナとして利用できるため，FET を埋め込むだけでよい．攻撃はターゲットに対して搬送波となる電波を送信し，その反射波を受信・復調することで実現する．電波の送受信はソフトウェア無線機と PC を組み合わせることで実現できる．攻撃者はアンテナ，ソフトウェア無線機，PC を用意し，ターゲットから離れた場所から秘密裏に攻撃を行う．

RFRA においてターゲットに埋め込むハードウェアトロイはシンプルで小型な回路であり，コストも低い．したがって RFRA が現実に実行されるリスクは十分にある．しかし RFRA による攻撃が現実的な環境下においてどの程度有効であるか，すなわち攻撃がもたらす脅威の実現可能性に関しては体系的な調査がない．本研究では RFRA が現実的な環境下で実行できるかということに主眼を置き，特にターゲットと攻撃者の距離，およびターゲットとなるデバイス上で扱う内部信号のデータレートに着目して，実験評価を行った．RFRA のターゲットとしてはケーブルを通じて平文で信号を送受信するデバイスを想定し，ケーブル中にハードウェアトロイを埋め込んだ．後に議論するように RFRA は高周波を扱うことができるハードウェア無線装置を利用することによって高いデータレートのターゲットを攻撃できるが，本研究はより実現性が高いアプローチとして，ソフトウェア無線による比較的低コストで入手可能な機材を利用する．

実験では攻撃者からターゲットまでの距離，およびターゲット内部信号の通信速度の 2 点に着目して攻撃の成否を評価した．この結果，距離に関する実験では，最大で 10 m の距離で攻撃が成功することを明らかにした．攻撃者がターゲットから 10 m 程度まで離れることができれば攻撃のセットアップの制約が少なくなり，状況に応じて最適な場所から攻撃を行うことができる．また通信速度に関する実験では，およそ 10 Mbps までの内部信号を反射波から復元することができた．USB キーボードやマウスで使われる規格は Low Speed モードと呼ばれ，通信速度は 1.5 Mbps である．つまり USB ケーブルにハードウェアトロイを埋め込めば RFRA によって USB キーボードの通信を盗聴し，例えば入力パスワードを盗み取ることができる．これらの攻撃を実現するのに用いた機材は総額で 50 万円程度であり，コストの観点からも実現可能性は高い．我々はこれらの結果より，RFRA は現実の脅威であると結論づけた．

2 章では関連研究を示す．3 章では RFRA の原理について説明を行う．4 章では実験のセットアップの詳細と，得られた結果を示す．5 章では実験を通じて明らかになったリスク，RFRA の制約，機材コストが無視できるケースについて議論を行う．最後に 6 章にて本論文のまとめを述べる．

2. 関連研究

RFRA が広まった経緯と現在までの関連研究について述べる．RFRA は広義には電磁波解析によるサイドチャネル攻撃に分類されるが，アクティブな攻撃である点が一般的なサイドチャネル攻撃とは異なる．一般的な電磁波解析によるサイドチャネル攻撃は対象から意図せず漏えいする電波を受信することで情報を取得する．しかし RFRA はターゲットに対して電波を照射し，その反射波を利用して情報漏えいさせる．ただしターゲットに対しては予め攻撃に必要な仕掛けをしておく必要がある．このように攻撃者が何らかのアクティブなアクションを起こすことにより行われるサイドチャネル攻撃に関する文献としては [1], [2] が挙げられる．[1] ではアクティブな攻撃方法を数例挙げ，また CIA はそのような攻撃を利用している可能性があると述べている．

2013 年 12 月に Edward Snowden がリークした文章群の中に United States National Security Agency (NSA) Advanced Network Technology (ANT) カタログ [3] と呼ばれる文章が含まれていた．NSA ANT カタログには ANGRYNEIGHBOR と呼ばれる技術が存在し，これは RFRA の原理に関するものである．このリークにより様々な技術

[1] 早稲田大学
Waseda University
[2] 仙台高等専門学校
National Institute of Technology, Sendai College
[3] 奈良先端科学技術大学院大学
Nara Institute of Science and Technology
[a)] wakabayashi@goto.info.waseda.ac.jp

が広まり，それらを実際に行うハッカーコミュニティも現れた [4], [5]．NSA Playset [4] の Micheal Ossmann はソフトウェア無線（SDR: Software Defined Radio）を利用した RFRA を行い，情報漏えいが可能なことを示した [6]．ターゲットには電界効果トランジスタ（FET）とダイポールアンテナからなる回路を仕掛けることで攻撃を行った．

また星野ら [7] は，今まで RFRA の成功例だけ報告され曖昧であった攻撃の成功条件について Ossmann の実装をもとに，実験により攻撃の成功条件を明らかにした．衣川ら [2] はターゲットそのものをアンテナとして利用することで Ossmann の実装を単純にし，RFRA がより現実的なものになることを示した．具体的にはターゲット信号が流れるケーブルのシールド線と信号線を FET を介して接続し，シールド線そのものをダイポールアンテナとして利用するという実装である．表面実装の FET は非常に小さく，製造時に埋め込んだ場合ターゲットの所有者は仕掛けがされていることに気付くのが難しい．

本研究は [7] で明らかになった攻撃成立条件を拡張し，実世界での実用性評価に焦点を置いた．実装面では [2] のターゲットケーブル内に FET が仕込まれた実装を利用した．また PS/2 キーボード（16 kbps）に対して行われてきた攻撃実験から，より高周波な信号への攻撃について実験を行った．

3. 電波再帰反射攻撃の原理

本章は電波再帰反射攻撃（RFRA）の原理を簡単に説明する．攻撃シナリオの概念を**図 1** に示す．RFRA はアクティブなサイドチャネル攻撃であり，攻撃者が外部から標的に対して能動的に電波を照射し，反射波を解析することで標的内部の信号を盗聴することが目的である．攻撃システムは電波の照射および反射波の受信・復調を行う攻撃部とハードウェアトロイが埋め込まれたターゲット部の 2 つから成る．攻撃者は事前にターゲットにハードウェアトロイを埋め込み，ターゲットの近傍から攻撃を行う．

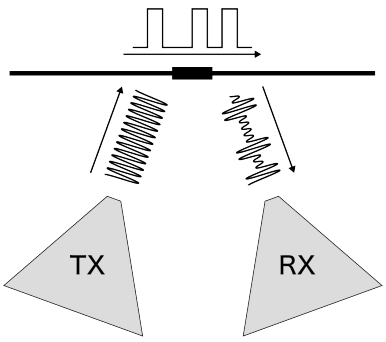


図 1 電波再帰反射攻撃の概要

図 2 にハードウェアトロイの回路図を示す．同軸ケーブルの外部導体であるシールド線を途中で切断し，両端をそれぞれ FET のソースとドレインに接続する．ゲートはケーブルの信号線 (すなわちターゲット信号が流れる線) に接続する．このように通信ケーブル上に FET を取り付けることにより，ケーブルそのものをハードウェアトロイにしている．

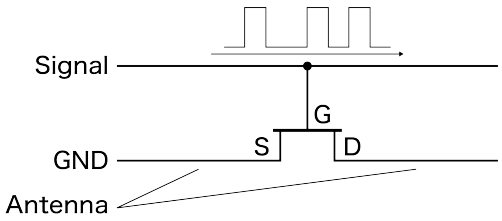


図 2 ハードウェアトロイの回路

次のような仕組みにより，反射波は照射した電磁波を搬送波としたターゲット信号による A M 変調波となる．まず，ケーブルのシールド線は取り付けた FET チップを境界としてダイポールアンテナと等価な構造を持っている．ターゲットに電波を照射するとアンテナ，すなわちシールド線に誘導電圧が発生する．この電圧は FET のゲートに印加されるターゲット信号電圧に比例して変化する．そのため，照射した電波がアンテナに誘導した電圧はターゲット信号電圧によって AM 変調される．そしてアンテナは AM 変調された信号を反射波として放射する．最終的に攻撃者は反射波を受信し，AM 復調することでターゲット信号を得ることができる．

照射する電波の周波数はアンテナの共振周波数となる．ターゲットが直線状であり，その中央に FET が取り付けられている場合は理想的なダイポールアンテナと見ることができる．したがってターゲット全体の長さが半波長となる周波数の電波を照射すればよい．またはその 3 倍，5 倍といった奇数倍の周波数でも共振するためより高周波な電波を照射しても動作する．ただしこれらはターゲットが直線状であると仮定した場合である．ケーブルをターゲットとする場合はその時々の形状や素材、設置場所によって共振周波数が影響を受けるため，厳密な共振周波数の計算は困難である．さらにはケーブルは何かしらのデバイスに接続され使用されるため，接続先のデバイス内の回路がアンテナとして動作すれば共振周波数は変化する．

4. 実験

本章では RFRA が成功する距離およびターゲットの通信速度を実験的に明らかにすることを狙いとする．はじめに 4.1 節 では実験のセットアップおよび作成したハードウェアトロイを示す．つぎに 4.2 節では攻撃可能な距離を調査した実験結果を示す．最後に 4.3 節では攻撃可能なターゲット信号の最大通信速度を調査した実験結果を示す．

4.1 実験セットアップ

図 3 に実験系の構成を示す．送受信の 2 つのアンテナは先端の距離が 1 m で固定し距離に応じて先端がハードウェアトロイの中心を向くように設置した．アンテナとターゲットはダンボールで作成した台の上に設置した．アンテナは真っ直ぐ伸ばした形状にした．これは実験系内に金属が存在すると攻撃の成否に影響をおよぼすためである．実験では送受信アンテナとターゲット間の距離，ターゲット信号の周波数の 2 つの観点から RFRA の評価を行った．

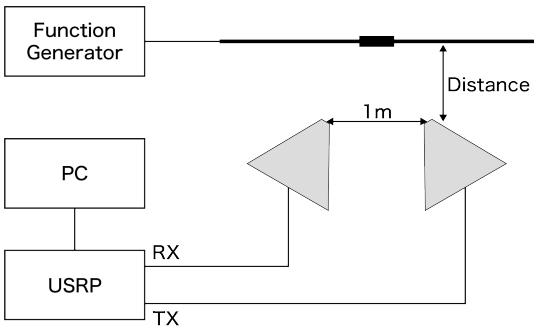


図 3 実験系の概要．

実験に使用した機材の一覧を**表 1** にまとめた．搬送波の送信および反射波の受信には SDR（Software Defined Radio）を利用する．利用した SDR (USRP) は全二重通信が可能であり，送信と受信は独立したアンテナを用いる．

SDR は信号処理をソフトウェアで行うシステムであり，処理内容を柔軟に変更することができる．**表 2** には攻撃者が SDR の駆動に用いる PC のスペックと使用した SDR ソフトウェアツールキットを示す．SDR を駆動するソフトウェアは GNU Radio [8] を利用した．GNU Radio を用いて照射波の生成および反射波の AM 復調処理を行う．SDR は PC と接続して利用し，受信した電波を PC に取り込む機能と電波を送信する機能を備えている．

ターゲットは一般的な通信ケーブルを想定し，同軸ケーブルに高周波向けの FET である高電子移動度トランジスタ（HEMT）を取り付けてハードウェアトロイとしたものを利用した．HEMT チップが取り付けられたターゲットケーブルを**図 4** に示す．ケーブルの全長を 1 m とし，ケーブルの中央に HEMT チップを取り付けた．ターゲットの内部信号はファンクションジェネレーターの任意波形機能を利用して生成した．

実験に利用するターゲット信号とハードウェアトロイの特性に関する測定結果を**図 5** に示す．**図 5(a)** はターゲット信号として意図した信号の理想的な波形である．ファンクションジェネレータはこのような信号を発生するように設定した．ファンクションジェネレータが出力した信号をオシロスコープで直接観測した結果を**図 5(b)** に示す．信号の電圧は 3 Vpp で周波数は 2 Mbps になるよう設定した．ハードウェアトロイを埋め込んだケーブル上で実際に流れる信号を**図 5(c)** に示す．これは**図 6** で示すようにハードウェアトロイを通してオシロスコープで観測した．ハードウェアトロイが受信する信号はファンクションジェネレータが生成する信号と比べて歪むことがみてとれる．

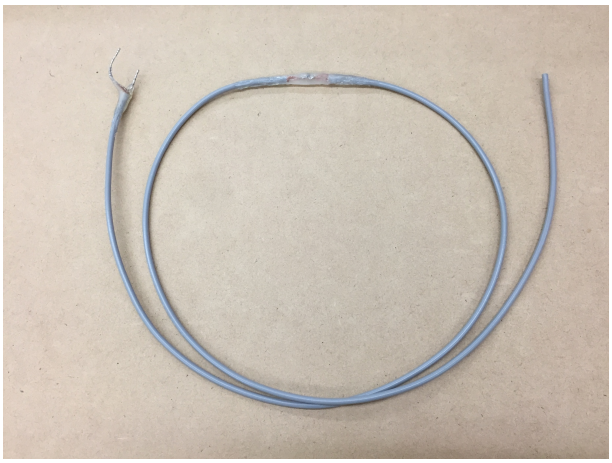


図 4 ハードウェアトロイが仕掛けられたケーブル

表 1 実験で使用した機材

機材	型番
送受信アンテナ	Ettus Research LP0410
ソフトウェア無線機	USRP N210
ファンクションジェネレータ	AFG3102
オシロスコープ	MSO4054
攻撃用 PC	ASUS ROG G752VS
HEMT (ハードウェアトロイ用)	ATF-54143

表 2 SDR 環境

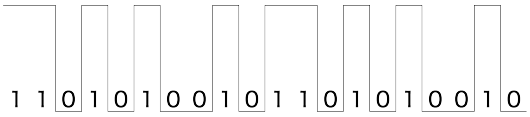
OS	Windows 10
SDR ソフトウェア	GNU Radio 3.7.11
CPU	Core i7 7700HQ 2.8 GHz/4 Core
RAM	32 GB

4.2 ターゲットまでの距離

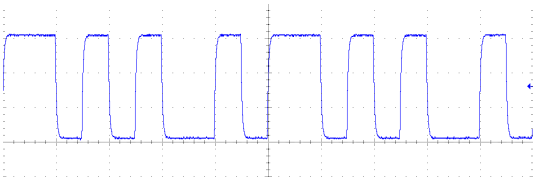
送受信アンテナとターゲットの距離を 1 m ずつ変化させ，距離と攻撃の実現可能性の関係について実験を行った．照射する電波の強度は使用した SDR の最大強度に設定した．ターゲット信号は 3 Vpp のデジタル信号を想定し，“1101010010” の 10 bit を繰り返す信号とした．信号周波数は 2 Mbps，電圧はローレベル 0 V，ハイレベル 3 V となるように設定した．図 5 に示す波形と同一である．SDR のサンプリングレートは 10 MS/s とした．**表 3** に実験条件をまとめて示す．

表 3 実験条件

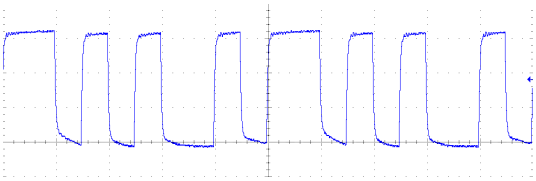
ターゲットとの距離	1 m ～ 11 m（1 m 刻み）
ターゲット信号電圧	3 Vpp
ターゲット速度	2 Mbps
サンプリングレート	10 MS/s



(a) 理想的な波形



(b) 直接観測した波形



(c) ハードウェアトロイを通して観測した波形

図 5　ファンクションジェネレータの波形

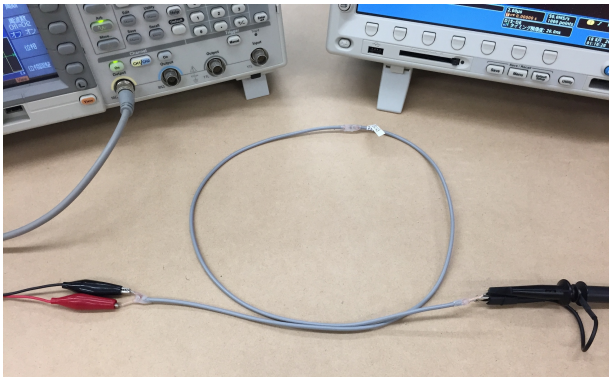


図 6　ターゲットとなるケーブルを実際に流れる信号の測定.

図 7 にターゲットまでの距離が 1，3，5，7，10，11 m のときに観測した波形を示す．図中に観測した信号波形をビット列にデコードした結果を記しており，上側に書かれたビットは正しくデコードできた例，下側に書かれたビットはエラーとなった例を示す．距離が大きくなるほど波形が大きく歪み，SNR が高まることがみてとれる．また，今回の実験セットアップでは攻撃可能な距離は 10 m 以内であった．10 m では，図に示した範囲内で 31 bit 中 2 bit の誤りが発生していおり，このときのビットエラー率は 6.5 %となる．11 m ではターゲット信号が確認できず，攻撃に失敗した．

フリスの伝達公式が示すように，自由空間においては電波の受信強度は距離の 2 乗に反比例する．このため 10 m と 11 m という 1 m の差でも受信強度が大きく下がり攻撃の成否が分かれたと考えられる．この仮説を検証するため，距離と反射波の受信強度の関係を調べた．**図 8** と**図 9** に実験結果を示す．図 8 では 100 bits 分の盗聴信号を示しており，上から順に距離を 1，3，5，7，10，11 m とした際の観測波形に対応する．Y 軸は GNU Radio により AM 復調された信号の振幅であり，ハードウェアトロイから反射してきた電波の受信強度を意味する．図 9 は 1 m における振幅を 1 とした場合の距離ごとの 振幅上限値の変化を示している．ここで振幅上限値とは図 8 で波形の上限付近に引かれた線の数値を示す．紙面の都合上 2，4，6，8，9 m のケースは省略したが，同様の結果を得ている．1 m から 2 m では振幅が大きく減衰しているが，その後は大きな減衰が見られない．特に 4，5，6 m では振幅が大きくなっているが，これは柱や壁などに起因する環境依存の現象であると考えられる．図 8 では 10 m と 11 m では振幅に大きな差が現れている．振幅が距離の 2 乗に反比例していない理由についてはさらなる調査が必要である．考えられる理由の 1 つとして，1 m と 2 m における反射波の受信強度が弱かった可能性がある．

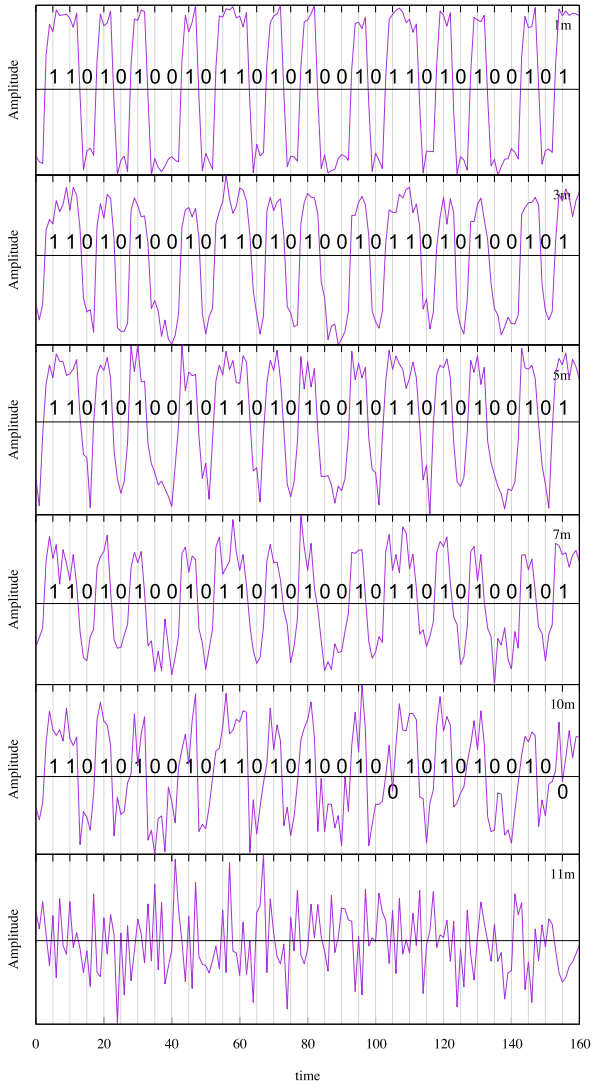


図 7　ターゲットまでの距離が 1，3，5，7，10，11 m の観測波形

表 4 に，距離毎に攻撃に成功した照射した電波の周波数を示す．ダイポールアンテナはその全長を半波長とする電

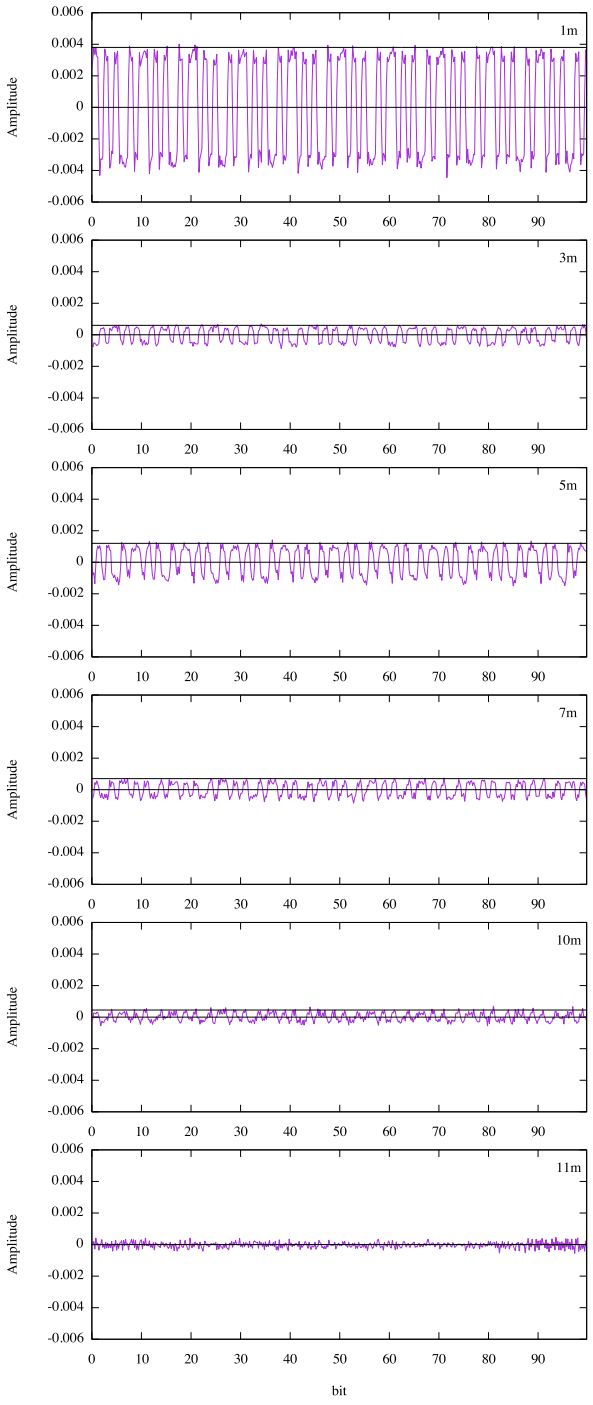


図 8 距離ごとの受信振幅

波と共振するため，今回実験に使用した 1 m のターゲットの場合およそ 150 MHz の電波と共振する．理論的には 1 m のダイポールアンテナは 150 MHz を基準として 3 倍，5 倍の奇数倍の周波数で共振するが，ファンクションジェネレータが接続されているため実質のアンテナ長が異なるため共振周波数も変化する．実験では 150 MHz の 4 倍である 600 MHz を中心に攻撃が成功する周波数を調べた．攻撃に成功した周波数は最大で 70 MHz の差があった．ただしこの差は距離とは相関がなく，アンテナの形状の変化

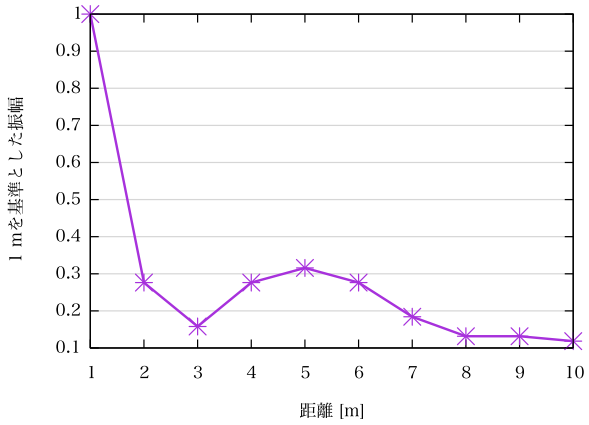


図 9 1 m での盗聴信号の振幅を 1 とした距離ごとの盗聴信号の振幅

によるものであることに注意する．距離を変える際にターゲットの形状や，ターゲットとファンクションジェネレータをつなぐケーブルの形状が変化したため結果として共振周波数が変化した．RFRA は形状の変化に大きな影響をうけることが分かった．

4.3 ターゲット信号の周波数

RFRA で読み取れるターゲット信号の周波数の限界を調査する実験を行った．送受信アンテナとターゲットの距離は 1 m で固定とし，ターゲット信号の周波数を変化させた．ターゲット信号は 1 Mbps，5 Mbps，10 Mbps，20 Mbps の 4 つの周波数で実験を行った．SDR のサンプリングレートは 25 MS/s とした．**表 5** に実験条件をまとめて示す．

ターゲット信号周波数がそれぞれ 1 Mbps，5 Mbps，10 Mbps のときの観測した波形を**図 10**，**図 11**，**図 12**，に示す．各図の上部は，ファンクションジェネレータで生成した信号をハードウェアトロイを埋め込んだケーブルを通して観測した信号の波形であり，下部は攻撃によって観測した波形である．照射した電波の周波数は 771.2 MHz である．実験では 10 Mbps までの信号の盗聴に成功した．SDR のサンプリングレートが 25 MS/s であるので，盗聴可能な信号の最大周波数はサンプリング定理より 12.5 MHz 未満である．20 Mbps の矩形波は最大で 10 MHz の矩形波から構成されているためサンプリングレート 25 MS/s では盗聴の限界に近い．実験では 25 MS/s で 20 Mbps の信号の盗聴を試みたが失敗したため，ハードウェアの限界により理論よりも実際に盗聴可能な周波数は低いと考えられる．

5. 議論

本研究では比較的低コストで調達できる機材を利用して攻撃の実用性を評価した．本章では実験により明らかになった攻撃の脅威や，RFRA の応用として考えられる実アプリケーションへの攻撃について考察する．また，機材調

表 4　照射した電波の周波数

距離 [m]	1	2	3	4	5	6	7	8	9	10
周波数 [MHz]	607.2	600.00	600.00	676.0	595.4	657.6	652	679.8	588.4	650

表 5　実験条件

ターゲットとの距離	1 m
ターゲット信号電圧	3 Vpp
ターゲット速度	1 Mbps, 5 Mbps, 10 Mbps, 20 Mbps
サンプリングレート	25 MS/s

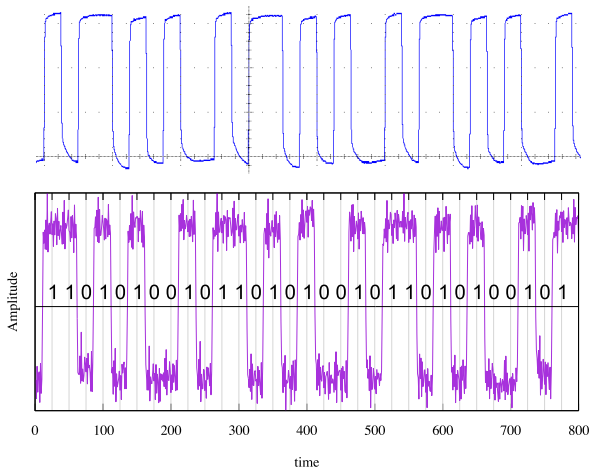


図 10　1Mbps の観測波形

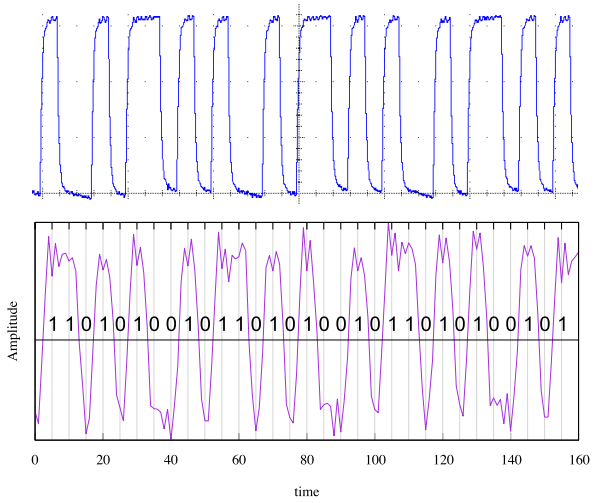


図 11　5Mbps の観測波形

達のコストに制約がない場合に可能となる攻撃の限界についても述べる．

5.1　攻撃の実用性

今回の実験セットアップで使用した機材は 50 万円以内で調達可能であり，コストの観点において実用的 (すなわち費用対効果が高い) といえる．USRP は 20 万円程度で購入が可能であり，また 20 万円程度のノート PC があれば SDR の処理は十分に可能である．その他は SDR に接続するログペリアンテナと SMA ケーブルを用意すればよい．

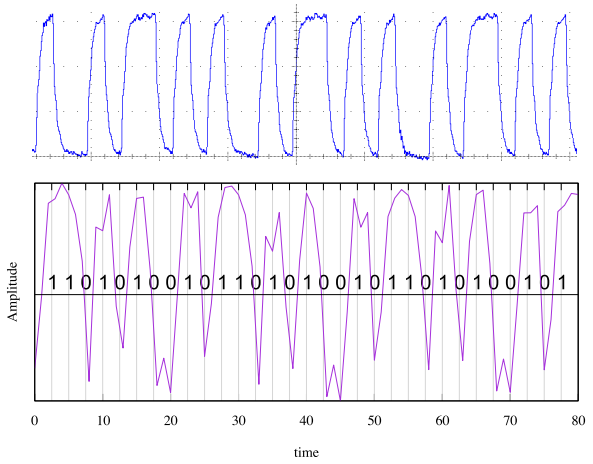


図 12　10Mbps の観測波形

実験の結果，ターゲットからは 10 m 程度離れることができるため，様々な攻撃シナリオが成立する．例えばターゲットの所有者に気づかれないよう少し離れた死角や物陰にアンテナを隠すアプローチが考えられる．ターゲット信号も 10 Mbps まで盗聴が可能であるため USB 2.0 で策定された High Speed モード (480 Mbps) 以上の通信を盗聴することはできないが，キーボードやマウスで使われている Low Speed モード (1.5 Mbps) は十分に攻撃可能である．これはキーボードで入力したパスワードが盗み取られることを意味する．

ターゲットに埋め込むハードウェアトロイそのものは受動的な回路であることが RFRA の大きな特徴である．すなわち攻撃者が能動的に電波を照射しなければ反射波は発生しないため，攻撃時以外は電波が漏えいしていることを検知できない．他にも同軸ケーブルのシールド線のようなアンテナの代わりになるものがターゲット自体に存在する場合，小型の FET を取り付けるだけでターゲットをハードウェアトロイ化できる利点もある．表面実装用の FET のサイズはとても小さいため，製品として違和感がないように，または気付かれないように FET を取り付けた通信ケーブルの製造なども可能である．

5.2　実アプリケーションへの攻撃

今回の実験ではデジタル信号のみをターゲットとしたが，アナログ信号をターゲットとすることも可能である．アナログ信号の代表として音声信号が挙げられる．音声信号の周波数はは人の可聴域に設定されるため，高々 40 kHz 程度である．5 MHz の矩形波への攻撃が成功していることを考えると 40 kHz への攻撃はより簡単である．

アナログの映像信号である VGA はピクセルあたりのク

ロックスピードは 25.175 MHz である．おおよそ 25 MHz の信号に対して攻撃を行うことができればよいため，今回の実験で使用した機材よりも高性能な機材を用意することで攻撃が実現できる可能性がある．ただし VGA では RGB の 3 色の通信ケーブルが存在するため，同時に 3 本のケーブルに対して攻撃を行う方法を検討しなければならない．

5.3 機材の制約がない場合の限界

手軽に入手可能な機材を使用した場合のリスクについて述べてきたが，その制約がない場合にどの程度まで攻撃の限界が広がるか検討を行う．USRP のサンプリングレートは 50 MS/s が最高であるため，サンプリング定理により復元可能な信号周波数は 25 MHz が限界である．しかし，高価なオシロスコープであれば数 GS/s から数百 GS/s といった高速なサンプリングレートを備えており，そのような高速サンプリングが技術的には可能であることが分かる．HEMT と呼ばれる高周波に特化した FET は数 GHz までの帯域を持っているため，ハードウェアトロイは数 GHz 程度までの信号を変調できる可能性がある．高周波に対応可能な専用ハードウェアを製造できれば盗聴可能なターゲット信号の周波数限界が大きく広がると考えられる．

5.4 攻撃が難しい点

RFRA において最も難しいのは照射すべき電波の周波数を決定する部分である．照射する電波の周波数はターゲット側のアンテナが持つ特性インピーダンスによって決定される．しかしこの特性インピーダンスはターゲットの形状によって大きく変化する．ターゲットがケーブルといった形状が変化するもので，なおかつ頻繁に形状が変化する場合，例えば所有者がターゲットを身につけていると照射すべき電波の周波数が変化し続けるため攻撃が難しくなる．攻撃にはターゲットの形状が変化しないという条件が必須となる．

6. まとめ

本研究では電波再帰反射攻撃の実用性を実験的に評価した．本研究のセットアップは 50 万円程度のコストで機材を揃えられること，および SDR を利用することで専用ハードウェアの設計をしなくても攻撃が可能であることに利点がある．SDR の利用によって専用ハードウェアの開発が不要になるだけでなく，攻撃が柔軟になる利点もある．SDR を駆動する PC 上で復調した盗聴波形をリアルタイムで確認することが可能であるため，頻繁に変化する最適な照射電波の周波数の追従も容易に実現できる．このようなセットアップを使うことにより 10 Mbps 程度までの信号であれば盗聴可能なことが示された．これは Low Speed モードを利用する USB キーボードを十分に攻撃可能な通信レートである．キーボードへの攻撃が成功すればパスワード等の機密情報の入力を盗聴できるため，大きな脅威である．実際の USB キーボードに対して RFRA を適用した実験評価は今後の課題である．また，音声などの通信レートが低いアナログ信号への攻撃も可能であり，実機による評価も今後の課題としたい．

一方で照射すべき電波の周波数がターゲットの形状に左右されるため攻撃をする際にある程度のチューニングが必要である点も明らかにした．アンテナとして動作する回路の形状と周波数の関係，壁越しの攻撃成否，その他物理的環境に依存する攻撃に影響を与える要因についてはさらなる研究の余地がある．

参考文献

[1] Anderson, R. J.: *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Publishing, 2 edition (2008).

[2] Kuhn, M. G. and Anderson, R. J.: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations., *Information hiding*, Vol. 1525, Springer, pp. 124–142 (1998).

[3] NSA ANT Catalog : `https://www.eff.org/files/2014/01/06/20131230-appelbaum-nsa_ant_catalog.pdf`.

[4] NSA Playset: `http://www.nsaplayset.org/`.

[5] GBPPR TAWDRYYARD Experiments: `http://gbppr.dyndns.org/~gbpprorg/mil/photoanglo/tawdryyard/index.html`.

[6] DEF CON 22 - Michael Ossmann - The NSA Playset: RF Retroreflectors : `https://youtu.be/mAai6dRAtFo`.

[7] 遼　星野, 昌宏衣川, 優一　林, 達哉　森：電波再帰反射攻撃の攻撃成立条件評価，コンピュータセキュリティシンポジウム 2016 論文集，Vol. 2016, No. 2, pp. 466–473 (2016).

[8] GNU Radio: `https://www.gnuradio.org/`.