UNICESUMAR - CENTRO UNIVERSITÁRIO DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS TECNOLÓGICAS E AGRÁRIAS
CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE

TEMPEST: Still a Signal Problem

IAGO DA COSTA OLIVEIRA

MARINGÁ – PR
2022

Iago da Costa Oliveira

TEMPEST: Still a Signal Problem

Artigo apresentado ao Curso de Graduação em Engenharia de Software da UNICESUMAR – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharel em Engenharia de Software, sob a orientação do Prof. M.sc. Aparecido Vilela Junior.

MARINGÁ – PR

2022

FOLHA DE APROVAÇÃO

IAGO DA COSTA OLIVEIRA

TEMPEST: Still a Signal Problem

Artigo apresentado ao Curso de Graduação em Engenharia de Software da UNICESUMAR – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharel em Engenharia de Software, sob a orientação do Prof. M.sc. Aparecido Vilela Junior.

Aprovado em: ____ de _____ de _____.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

TEMPEST: Still a Signal Problem

Iago da Costa Oliveira

RESUMO

TEMPEST é uma vulnerabilidade de hardware que explora emanações não intencionais emitidas por dispositivos eletrônicos. Desde 1914 já se possui conhecimento sobre esse tipo de vulnerabilidade. Neste documento serão apresentados alguns testes que foram realizados com o objetivo de entender como esta vulnerabilidade funciona e o quão acessível é a sua prática. Com um dispositivo SDR e uma antena foi possível coletar informações emanadas por um monitor e até mesmo replicar a tela do monitor com o software TempestSDR. Concluindo algumas hipóteses de que a vulnerabilidade é de fato acessível e pode ser uma grande ameaça para diversos setores, podendo ser uma ameaça ainda maior com o avanço de tecnologias IoT e cidades inteligentes.

Palavras-chave: Emanações Eletromagnéticas. SDR. Vulnerabilidade de Hardware.

TEMPEST: STILL A SIGNAL PROBLEM

ABSTRACT

TEMPEST is a hardware vulnerability that exploits unintentional eletromagnetic emanations from electronic devices. This vulnerability is known since 1914. In this document will be presented some tests that were carried out in order to understand how this vulnerability works and how accessible it is to perform this kind of attack. With an SDR dongle and an antenna was possible to collect emanated information from a monitor and using TempestSDR software the monitor screen was replicated. Concluding that this vulnerability is indeed accessible and can be a major threat to several sectors, and can be an even greater threat with the advancement of IoT technologies and smart cities.

Keywords: Eletromagnetic Emanations. Hardware Vulnerability. SDR.

SUMÁRIO

1 INTRODUÇÃO

O uso de dispositivos eletrônicos está presente na vida das pessoas como algo quase que obrigatório, já que hoje os utilizamos para nos conectar com quem está distante, estudar, se divertir e até mesmo para pagar as contas. Mas nem tudo é solução, pois, com o avanço e a disseminação da tecnologia também são criados novos problemas. Sempre conectados, desta forma, estamos vulneráveis a diversas ameaças, algumas conhecidas e outras que nem sabemos ainda.

Desde o início dos anos 1960, organizações militares já possuem conhecimento referente à emanações comprometedoras ou radiação eletromagnética, algo que não só interfere com a recepção de sinais de rádio, mas, também emana informações sobre os dados processados em forma de ondas. Também conhecido como emanações comprometedoras ou radiação TEMPEST. (KUHN, ANDERSON ,1998)

TEMPEST é um acrônimo para *Transient Eletromagnetic Pulse Emanation Standards*, que são padrões e contramedidas definidas pelo governo dos Estados Unidos com o intuito de proteger informação sensível de ser interceptada. (GARLICK, 2005)

Nos dias de hoje, diversas instituições e pessoas estão, de maneira não intencional, expostas a ataques TEMPEST. Esse tipo de ataque funciona por meio da captura de ondas ou radiações eletromagnéticas para reconstruir as informações vazadas. (AYDIN, 2019)

Ataques do tipo TEMPEST, muitas vezes, podem possuir um baixo custo para sua execução, porém a forma de se proteger pode acabar sendo custosa. Agência militares fazem uso da blindagem, ou seja, utilizam metais para revestimento de certas áreas ou até mesmo instalações. Outra forma de blindagem utilizada pelas agências é a proteção do próprio dispositivo, porém o preço dele acaba sendo altamente elevado e, dependendo, ele não se torna tão prático, como é o caso dos tipos móveis. (GOODMAN, 2021)

Neste projeto serão abordados alguns experimentos que foram utilizados para testar este tipo de vulnerabilidade. O estudo sobre TEMPEST começou por curiosidade e preocupação com a insegurança de hardwares e o avanço de tecnologias como cidades inteligentes e IoT. Deve-se ressaltar que os equipamentos utilizados não foram desenvolvidos para essa finalidade, mas, ainda assim, por possuirmos equipamentos de fácil acesso e baixo custo foi possível obtermos resultados interessantes.

2 EMANAÇÕES ELETROMAGNÉTICAS NÃO INTENCIONAIS

Dispositivos eletrônicos ou digitais, que utilizam eletricidade, estão sujeitos a emanações involuntárias, tendo em vista que uma corrente elétrica é um fluxo de partículas eletricamente carregadas, e uma tensão elétrica pode ser definida como uma concentração de cargas elétricas. Cargas elétricas criam campos elétricos ao seu redor, onde a intensidade é determinada pela intensidade da tensão, ou seja, quanto maior a tensão maior é a intensidade o que acaba gerando ondas eletromagnéticas.

Ataques do tipo TEMPEST fazem o uso de emanações eletromagnéticas liberadas por dispositivos eletrônicos, que por sua vez utilizam de correntes elétricas, o que leva a movimentação de partículas carregadas. Partículas carregadas em movimento criam campos magnéticos e a combinação de campos magnético e elétrico gera o que se conhece por campo eletromagnético. Quando qualquer componente do campo eletromagnético sofre alteração, ela é propagada formando o que se conhece por ondas eletromagnéticas. (KARLSSON, 2003)

Um melhor design, ou um design mais apropriado, pode reduzir sinais não intencionais emitido por um dispositivo, porém, ainda, existirá a emanação de sinais. Por existir esse tipo de emanação, é comum dispositivos eletrônicos interferirem com outros dispositivos. (GOODMAN, 2021)

Segundo a União Internacional de Telecomunicações, algumas maneiras de mitigação dessa vulnerabilidade são: Blindagem de instalações, Blindagem de equipamentos, Filtragem, Zoneamento, Soft Tempest e Camuflagem.

- Blindagem de instalações: consiste em revestir locais com materiais metálicos. É considerada a forma mais confiável de prevenção, porém é altamente custosa de aplicar.
- Blindagem de equipamentos: segue a mesma ideia de revestimento com materiais metálicos, porém é aplicada diretamente nos equipamentos. Mesmo assim, a emanação ocorrerá em diversos pontos como impressoras, periféricos, computadores, cabos, entre outros. Entretanto, é difícil realizar a blindagem onde existe a necessidade da interação como telas, teclados, mouses, painéis touch etc.; além dos dispositivos blindados serem mais custosos e pesados.
- Filtragem: inserir filtros em cabos de interface, principalmente, de vídeo. Também é efetivo contra as emissões eletromagnéticas, porém elas ainda continuam a irradiar a partir dos circuitos internos presentes nos dispositivos.

- Zoneamento: é uma política de distanciamento, permitindo a tomada de decisão com base no nível de cada zona. Desse modo, pode-se decidir a contramedida a ser utilizada. As zonas podem ser definidas como:
    - Zona 0: a mais de 100 metros de distância do sistema (fora da instalação);
    - Zona 1: de 100 metros a dez metros de distância do sistema (dentro da local);
    - Zona 2: de dez metros a um metro de distância do sistema (dentro da mesma instalação/estrutura);
    - Zona 3: A menos de um metro (dentro da mesma sala);
- Soft Tempest: software empregado como contramedida. A utilização das funções dele suavizarão fontes ou imagens e reduzirá a força da emanação quando aplicadas em telas.
- Camuflagem: trata-se da utilização de emissão propositais de sinais sem informação (chiado) para dificultar e ofuscar emanações comprometedoras. É uma contramedida de baixo custo, porém, deve-se tomar cuidado ao aplicar a técnica para que os sinais de camuflagem não interferiram com o funcionamento normal dos dispositivos próximos.

3 HISTÓRIA TEMPEST

Ataques que se aproveitam de ondas eletromagnéticas já são conhecidos há algum tempo, sendo utilizado militarmente por agências de inteligência para espionagem. Em 1914, teve-se relato da primeira exploração desse fenômeno, em que o exército britânico observou conversas cruzadas devido a vazamentos dos fios de telefones. A partir de então, foram criadas estações de escuta com o intuito de interceptar a comunicação inimiga. Porém, somente em 1967 esse tipo de vulnerabilidade foi apresentado ao público. (MARINOV, 2014)

A agência de segurança americana (NSA) realizou uma pesquisa em 1972 onde nomeou o problema como TEMPEST. O documento relata sobre um teste prático realizado pela companhia Bell Lab, uma fornecedora de dispositivos para criptografia. No teste, os engenheiros, que estavam em um edifício do outro lado da rua, a uma distância aproximada de 25 metros, gravaram e depois processaram, na forma de texto simples, sem nenhum tipo de criptografia, 75% dos sinais capturados por uma hora.

Nos dias de hoje esse tipo de vulnerabilidade ainda é uma realidade. Em 2012, Fürkan Elibol, Uğur Sarac e Işın Erer realizaram um estudo utilizando um dispositivo móvel de baixo custo para aplicar a técnica e demonstrar que o TEMPEST é uma grande ameaça. No estudo, a técnica foi executada em duas configurações diferentes: primeiramente, em um laptop a uma distância de três metros; e posteriormente, em um monitor LCD, a uma distância de 46 metros. Em ambos os casos foram bem sucedidos o que resultou na captura de uma imagem estável da tela.

Em 2014, Martin Marinov utilizou-se de um software chamado TempestSDR para replicar a imagem de um monitor que estava a uma distância de sete metros e possuía duas paredes entre o dispositivo de captura e o monitor. O software TempestSDR mapeou a intensidade do campo de um pixel para uma tonalidade de cinza, apresentando em tempo real a tela capturada.

4 MATERIAIS

Durante este projeto foram utilizados os segundos equipamentos e softwares:

- RTL-SDR;
- Monitor LG Flatron W1643C;
- Antena SMA 433 MHz 5dBi;
- Software SDR#;
- Software TempestSDR;

4.1 RTL-SDR

Scanner de rádio para computador, dispositivo utilizado para captura de sinal de rádio..

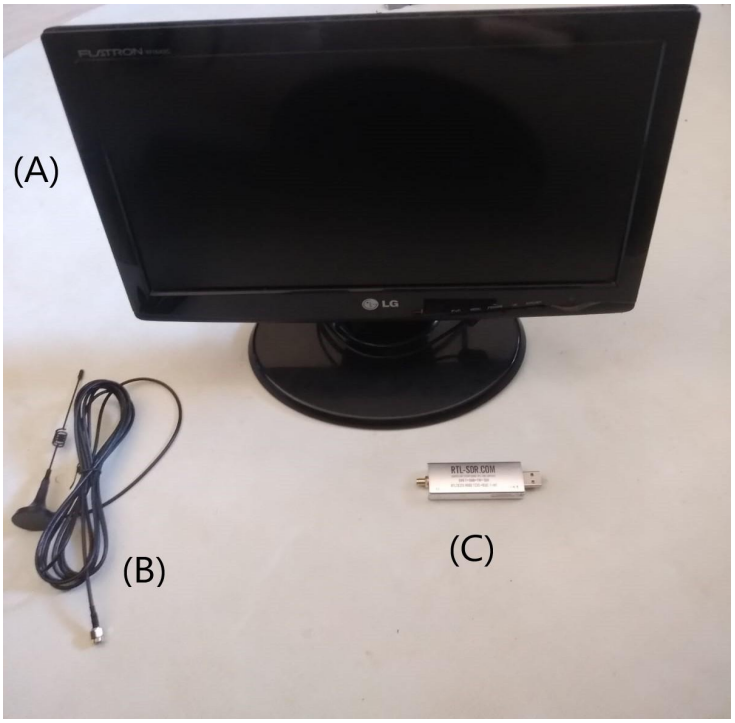
4.2 Software SDR#

SDR# é um software SDR (Software Defined Radio) compatível com RTL-SDR. Softwares SDR são programas que permitem o RTL-SDR funcionar como um receptor de rádio.

4.1 TempestSDR

É um software para a captura de vídeo de monitores, que utiliza um receptor SDR, explorando emanações comprometedoras de cabos que transmitem sinais de vídeo.

Foto 1 - Materiais utilizados



Fonte: Fotos do autor. / (A) monitor LG Flatron W1643C, (B) Antena SMA 433MHz 5 dBi, (C) Dispositivo RTL-SDR.

5 RESULTADOS E MOTIVAÇÃO

Com o crescimento da utilização de sistemas IoT (Internet das Coisas) e a crescente em cidades inteligentes, fez-me questionar se, realmente, estamos preparados e seguros, pois,

com os sistemas ainda vulneráveis, nossas vidas podem estar sujeitas a grandes impactos. Para responder ao questionamento, foram realizados dois testes: um para identificar o vazamento de informações por emanações via rádio, utilizando-se de um vídeo; e um segundo, utilizando-se a abordagem apresentada por Martin Marinov em sua pesquisa, com a dúvida de quão acessível seria aplicar uma técnica como essa.

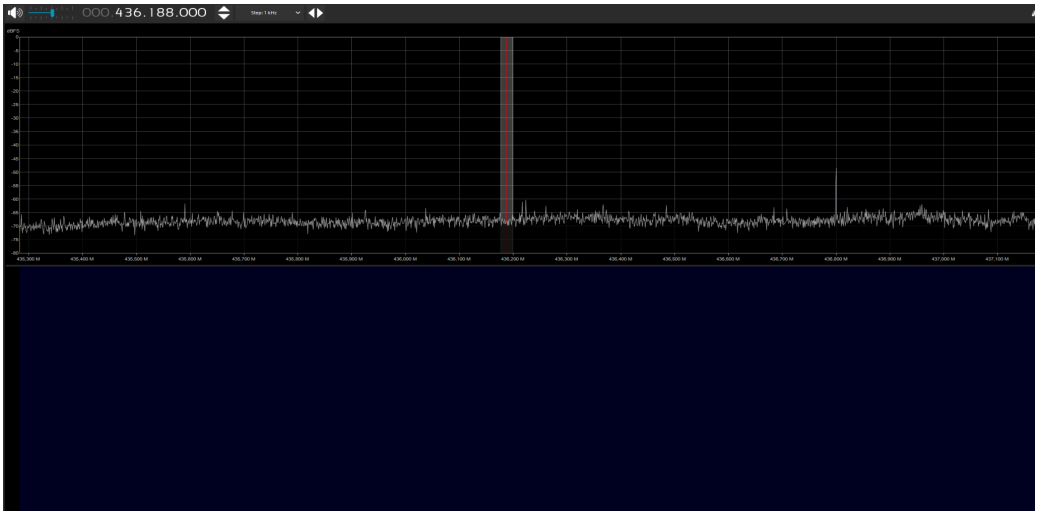
5.1 Configuração do teste

Com o monitor ligado, e apresentando uma imagem, posicionou-se a antena a uma distância de cinco centímetros da tela. A antena se conectava ao dispositivo RTL-SDR que, por sua vez, estava conectado a um computador.

5.2 Escutando emanações do monitor

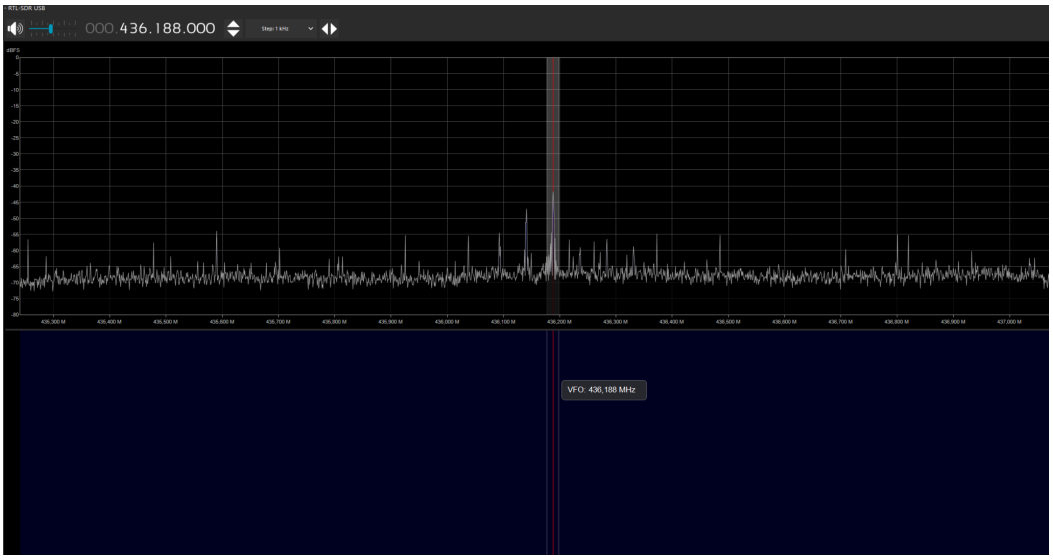
Utilizando-se a configuração mencionada anteriormente, colocou-se no monitor a exibição do vídeo “Tempest - Make Your Monitor Play Beethoven 2.0” que pode ser acessado no link <https://www.youtube.com/watch?v=DlVM9xqGKx8>. Em seguida, utilizando-se do software SDR# buscou-se a frequência que o monitor estava emanando de forma manual, ou seja, alterando-se o alcance da frequência no software para identificar alterações ou picos de sinais significativos. Ao chegar em aproximadamente 435.500 MHz, revelou-se uma mudança no sinal, conforme a imagem apresentada no monitor se alterava, como pode ser observado nas ilustrações abaixo.

Foto 2 - Frequência sem a imagem na tela



Fonte: Fotos do autor.

Foto 3 - Frequência com a imagem na tela



Fonte: Fotos do autor.

Em 436.188 MHz foi possível identificar o maior pico no sinal capturado. Escutar esta frequência propiciou ouvir a música “Für Elise” composta pelo compositor alemão Ludwig van Beethoven. Mesmo com um insignificante chiado de fundo, era claro que a configuração estava capturando o que era proposto no teste. Ao se modificar um pouco a configuração, e colocando a antena diretamente no cabo, foi possível ainda ouvir claramente a música sem sofrer alteração no pico do sinal capturado. O mesmo não se observou quando a antena, sem estar conectada ao cabo, permaneceu em igual distância afastada do monitor.

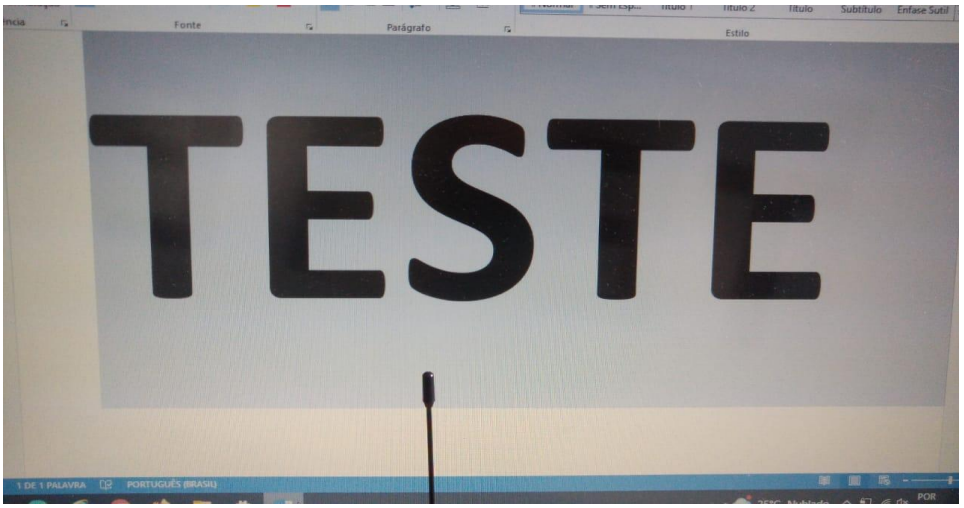
5.3 Abordagem de Martin Marinov

Com a proposta de capturar a tela em tempo real, foi utilizado a mesma configuração mencionada anteriormente, com o software TemprestSDR, disponibilizado no github do usuário eried no link <https://github.com/eried/Research/tree/master/HackRF/TempestSDR>. Antes de executar o teste foi necessário realizar uma alteração: com o arquivo TempestSDR aberto por meio do programa WinRar, excluiu-se o arquivo ExtIO_HackRF.dll e se adicionou o arquivo ExtIO_RTL2832 obtido no link <http://www.hdsdr.de/hardware.html>. Após as referidas operações foi possível selecionar a opção load ExtIO source que identificou automaticamente o dispositivo RTL-SDR.

Finalizando as configurações do software, foi necessário identificar, novamente, de maneira manual, a frequência com que a imagem emanava. Identificou-se diversas frequências tornando possível a observação da tela sendo capturada, porém, em 1.151.000 MHz, percebendo assim uma maior estabilidade.

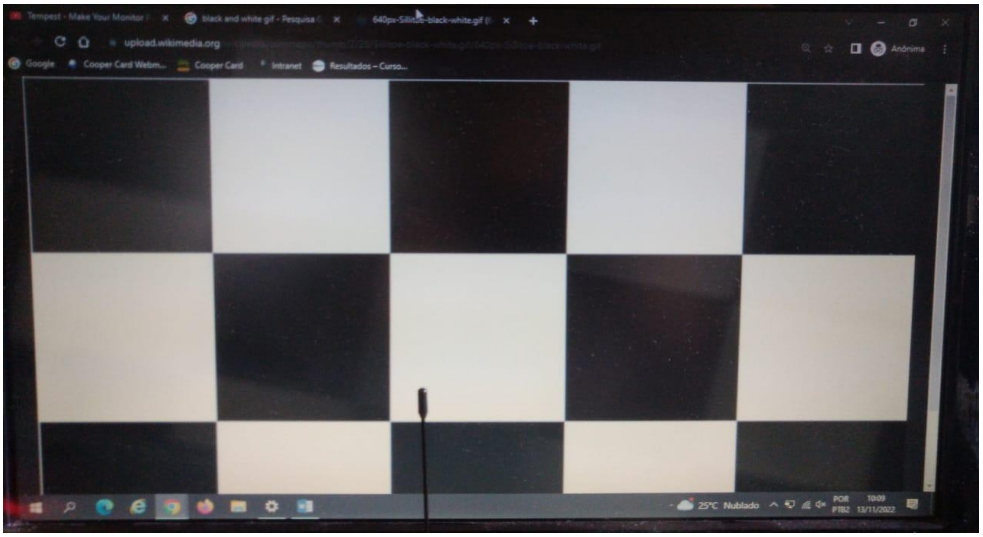
No monitor, projetou-se a apresentação de um texto de teste onde era exibida a palavra “TESTE” e outra imagem que consistia em um tabuleiro de xadrez, conforme é mostrado abaixo.

Foto 4 - Tela utilizada para captura com a escrita “TESTE”



Fonte: Fotos do autor.

Foto 5 - Tela utilizada para captura apresentando o tabuleiro de xadrez



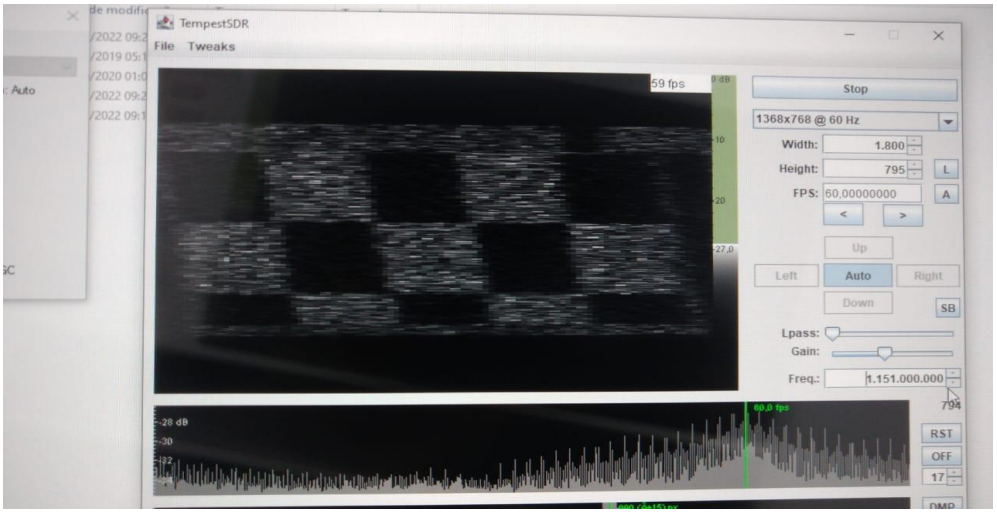
Fonte: Fotos do autor.

Foi possível identificar as telas capturadas, porém, a qualidade da captura não possuía tanta nitidez para se observar detalhes ou pequenas imagens da tela, conforme os resultados abaixo.

Foto 6 - Tela utilizada para captura apresentando o tabuleiro de xadrez

Fonte: Fotos do autor.

Foto 7 - Tela utilizada para captura apresentando o tabuleiro de xadrez



Fonte: Fotos do autor.

Os testes foram bem sucedidos, pois foi possível capturar as imagens desejadas e também distingui-las. Pode-se observar que a nitidez da imagem não foi alta, devido aos materiais utilizados. Certamente, um resultado melhor poder-se-ia obter utilizando-se uma antena com um ganho maior, ou um receptor mais potente, ou a adição de amplificadores, entre outras possíveis alterações na configuração do ataque.

6 CONCLUSÃO

TEMPEST é um tipo de vulnerabilidade que já se possui conhecimento há mais de um século, porém, devido à forma que os dispositivos eletrônicos são desenvolvidos, tornou-se algo árduo para se combater. Por falta de alternativas no desenvolvimento de dispositivos eletrônicos, essa vulnerabilidade está presente em nosso cotidiano. Mesmo com mais de um século, essa ameaça ainda continua sendo uma realidade e os danos e consequências que o TEMPEST pode causar são mitigados, não por causa de ferramentas e/ou pesquisas, mas sim, pela falta de conhecimento da população com relação a essa vulnerabilidade.

Durante o desenvolvimento do projeto foi realizado diversos testes que, mesmo não apresentando alta nitidez, se provaram bem sucedidos, demonstrando que de fato a tecnologia para a prática de ataques do tipo TEMPEST é acessível e que esta vulnerabilidade ainda é uma realidade, além de ser uma grande ameaça para setores que trabalham com informações sensíveis. Outro ponto importante é que esse tipo de ataque não deixa rastros, tornando quase que impossível determinar com que frequência ele ocorre.

Existem diversos tipos de vulnerabilidade de hardwares, o TEMPEST é um deles. Com o crescimento do uso de tecnologias IoT, principalmente, em cidades inteligentes, faz com que essas vulnerabilidades se tornem um risco ainda maior para a segurança não só individual como também para a segurança de uma nação.

7 REFERÊNCIAS

AYDIN. H. TEMPEST Attacks and Cybersecurity. **INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGIES - IJET**, v. 5, n. 2, p 100-104, set. 2019.

ECK, W. V. **Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?** 4. ed. Leidschendam: North-Holland, Computers & Security, 1985.

ELIBOL, F., SARAC, U., ERER, I.. **REALISTIC EAVESDROPPING ATTACKS ON COMPUTER DISPLAYS WITH LOW-COST AND MOBILE RECEIVER SYSTEM**. In: 20th European Signal Processing Conference (EUSIPCO), 27, agosto, 2012, Bucareste.

ESTADOS UNIDOS DA AMÉRICA. NATIONAL SECURITY AGENCY - NSA. **TEMPEST: A Signal Problem**, 1972.

GARLICK, Daniel. **TEMPEST And Electromagnetic Emanations Security: Is Not Only A Government Standard.** 2005. Disponível em: https://www.giac.org/paper/gsec/4287/tempest-electromagnetic-emanations-security-government-standard/106943. Acesso em: 06 out. 2022.

GOODMAN, Cassi. **An Introduction to TEMPEST**. 2021. Disponível em: https://sansorg.egnyte.com/dl/HrZNobu2Vo. Acesso em: 17 out. 2022.

International Telecommunication Union. **ITU-T K.115**: Mitigation methods against electromagnetic security threats, 2015.

KARLSSON. J. **TEMPEST Attacks - Using a simple radio receiver**. 2003. Tese de mestrado. (Mestre de Ciência em Ciência da Computação) - Instituto de Tecnologia de Blekinge, Ronneby, Suécia.

KUHN, M. G.. **Compromising emanations: eavesdropping risks of computer displays**. Cambridge: Universidade de Cambridge, 2003.

KUHN, M. G., ANDERSON, R. J. **Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations**.1998 In: Aucsmith, D. (eds) Information Hiding. IH 1998. Lecture Notes in Computer Science, vol 1525, 1998, Portland, p. 124-142.

LIU. Z. et al. **Screen Gleaning: A screen reading TEMPEST Attack on Mobile Devices Exploiting a Eletromagnetic Side Channel**. In: NETWORK AND DISTRIBUTED SYSTEMS SECURITY (NDSS) SYMPOSIUM, 23, fevereiro, 2021, Virtual.

MARINOV. M. **Remote video eavesdropping using a software-defined radio platform**. 2014. Dissertação de mestrado. (Mestre de Filosofia em Ciência da Computação Avançada) - Universidade de Cambridge, Cambridge, Reino Unido, 2014.