CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise de Sistemas

EMSEC (*Emissors Security - Tempest*):

Uma forma alternativa de invasão de sistemas

Danilo André Jorge Patrício

Americana, SP
2012

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Análise de Sistemas

EMSEC (*Emissors Security - Tempest*):

Uma forma alternativa de invasão de sistemas

Danilo André Jorge Patrício

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Análise de Sistemas da Fatec Americana, sob orientação do Prof. Dr. José Luís Zem.

Área: Segurança da Informação

Americana, SP
2012

FICHA CATALOGRÁFICA elaborada pela
BIBLIOTECA – FATEC Americana – CEETPS

Patrício, Danilo André Jorge
P341e EMSEC (Emissors Security - Tempest): uma forma alternativa de invasão de sistemas. / Danilo André Jorge Patrício. – Americana: 2012.
77f.

Monografia (Graduação em Análise de Sistemas e Tecnologia da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. José Luís Zem

1. Segurança em sistemas de informação I. Zem, José Luís II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Bibliotecária responsável Ana Valquiria Niaradi – CRB-8 região 6203

BANCA EXAMINADORA

Prof. Dr. José Luís Zem

Profa. Dra. Maria Cristina Aranda Batocchio

Prof. Ms. Clerivaldo José Roccia

AGRADECIMENTOS

A Deus, essencialmente, pela existência de tudo.

Aos meus pais e irmãos, por investirem em minha educação, cuidarem do meu sustento e compreenderem minha ausência.

Ao orientador e professores, pela paciência em acreditarem no meu objetivo.

Aos colegas de grupo, por manterem os trabalhos ativos em minha omissão.

Enfim, a todos que direta ou indiretamente contribuíram para a árdua conclusão deste trabalho.

“Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano.

Apesar do nosso intelecto, nós humanos — você, eu e todas as outras pessoas — continuamos sendo a ameaça mais séria à segurança do outro.”

Kevin D. Mitnick

RESUMO

O objetivo da pesquisa é apresentar uma metodologia para diagnosticar problemas de invasão de sistemas. Trata-se do método denominado *Tempest*, no qual é possível acessar informações de computadores que são fabricados com blindagem precária. Em virtude dessa falha, a emissão eletromagnética pode ser captada com instrumentos simples e de fácil acesso e assim, quebrar as barreiras físicas e lógicas como: controle de acesso, senhas e antivírus. As discussões sobre o uso dessa metodologia indicam que o domínio de mais uma camada relacionada à segurança é essencial para que o administrador de sistemas esteja atento às inúmeras possibilidades de invasão que podem comprometer a segurança da informação.

PALAVRAS-CHAVE: Segurança da informação, controle de acesso, emissão eletromagnética, blindagem.

ABSTRACT

The aim of this research is to present a methodology for diagnosing problems of systems intrusion. It refers to the method called Tempest in which it is possible to access information from computers that are manufactured with poor shielding. Because of this failure, the electromagnetic emissions can be captured with simple tools and easy access and thus to break down barriers both physical and logical as: access control, antivirus and passwords. Discussions about the use of this methodology indicate that the domain of another layer of safety-related systems is essential for the system administrator to be aware of the endless possibilities of intrusion that could compromise information security.

KEYWORDS: Information Security, access control, electromagnetic emission, shielding.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ABRICEM	Associação Brasileira de Compatibilidade Eletromagnética
ACA	Australian Communications Authority
ALS	Advanced Light Source
AM	Amplitude modulation
ANATEL	Agência Nacional de Telecomunicações
ANVISA	Agência Nacional de Vigilância Sanitária
APS	Advanced Photon Source
BBS	Bulletin board system
CBAC	Comitê Brasileiro de Avaliação da Conformidade
CC	Creative Commons
CD	Compact disc
CE	Consumer Electronics
CERT	Computer Emergency Response Team
CRT	Cathode ray tube
DIN	Deutsches Institut für Normung
DVD	Digital versatile disc
DVI	Digital visual interface
EHF	Extremely high frequency
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EMR	Electromagnetic radiation
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
HDCP	High-bandwidth digital content protection
HDMI	High-definition multimedia interface
HF	High frequency
IAB	Internet Architecture Board
IEC	International Electrotechnical Commission
IEE	Institute of Electrical and Eletronic Engineers
IEFT	International Engineering Task Force
INMETRO	Instituto Nacional de Metrologia, Normalização e Qualidade Industrial
IR	Infrared

ISO	International Standards Organisation
ITU-T	International Telecommunication Union
LASEC	LAboratoire de SÉcurité et de Cryptographie
LED	Light emitting diode
LCD	Liquid crystal display
LF	Low frequency
MD5	Message digest algorithm
MF	Medium frequency
MP3	Moving picture experts group - audio layer 3
MTSO	Mobile telephone switching office
NASA	National Aeronautics and Space Administration
NBR	Norma Brasileira
NSA	National Security Agency
PBAC	Programa Brasileiro de Avaliação da Conformidade
PC	Personal computer
PS/2	Personal system 2
RADAR	Radio detection and ranging
RAM	Random access memory
RCA	Radio Corporation of America
RFC	Request for comments
SBAC	Sistema Brasileiro de Avaliação da Conformidade
SHA	Secure hash algorithm
SHF	Super-high frequency
SONAR	Sound navigation and ranging
THF	Tremendously high frequency
TMDS	Transmition minimized differential signalling
UHF	Ultrahigh frequency
USB	Universal serial bus
UV	Ultraviolet
VGA	Video graphics array
VHF	Very high frequency

SUMÁRIO

1 INTRODUÇÃO

A exposição presente do trabalho de conclusão de curso mostrará o panorama da realidade sobre a segurança da informação adotada nas empresas e o impacto que as novas tecnologias acrescentam em benefício de seu negócio, contudo, essas tecnologias causam sérios prejuízos quando não adotadas precauções necessárias.

1.1 Objetivos

Nos dias atuais, as empresas, de modo geral, não consideram a Informação como um ativo, pois ainda não se atentaram ao risco de suas Informações serem violadas, roubadas ou mesmo perdidas. Para esclarecer sobre ativo, segundo a norma ABNT NBR ISO/IEC 27001:2006, ativo é qualquer coisa que tenha valor para a organização (ABNT, 2006). Já na norma ABNT NBR ISO/IEC 17799:2005, a Informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegido (ABNT, 2005). Na área administrativa, segundo Chiavenato (2005), o ativo mais importante para uma organização é o capital intelectual, aquilo que entra e sai pelas portas diariamente, ou seja, o conhecimento no qual as pessoas carregam em suas mentes. Pensando nisso, o propósito do trabalho é apresentar um aspecto distinto na abordagem de segurança da informação nas empresas, uma vez que todo sistema de segurança, por mais estruturado que seja, pode apresentar falhas.

Há inúmeras metodologias de invasão criadas praticamente todos os dias no mundo inteiro e acabam por fugir dos padrões conhecidos devido à criatividade e imaginação criadas pelas pessoas. O trabalho enfoca uma dessas metodologias: a captação de ondas eletromagnéticas de equipamentos eletrônicos nos quais transportam informações ou variações de frequência passíveis de serem decodificas. O desenvolvimento do trabalho improvisará uma simulação dessa metodologia mostrando a possibilidade de obter informação utilizando equipamentos corriqueiros e fácil acesso.

1.2 Justificativa

O profissional da área de segurança da informação, seja um administrador ou analista de sistemas, necessita ter a cada dia, uma visão global de toda infraestrutura de rede e

conhecer detalhadamente os caminhos pelos quais a informação percorre para que chegue ilesa ao seu destino sem que seja interceptada. Não basta mais somente manter todo o sistema ativo, disponível a qualquer momento e funcional. A exigência das empresas preocupadas com seus ativos é de proteger seus dados que trafegam constantemente pelas redes e armazená-los em segurança com a finalidade de futuras consultas.

Para satisfazer essas exigências e conservar o sistema livre de intrusões, o profissional de segurança deve estar sempre atualizado, conhecer todas as ferramentas distintas e recém-descobertas de invasão, participar de palestras sobre o assunto e investir em cursos de aperfeiçoamento. Além disso, implementar ou reavaliar a política de segurança da empresa, detectar brechas, sugerir mudanças eficazes e manter uma rotina de auditoria para confirmar se as políticas estão sendo aplicadas adequadamente.

1.3 Metodologia

O trabalho iniciará a partir de uma investigação do tema tomando por base a literatura de livros sobre Segurança da Informação, Redes de Computadores, Técnicas de Invasão, Criptografia, Perícia Forense, Engenharia Elétrica, Eletrônica e Física.

Também serão utilizados diversos documentos governamentais provindos de órgãos normativos, agências de segurança e de inteligência americanos e militares. Outra fonte fundamental serão os ensaios realizados por pesquisadores de universidades de vários países através de publicações de relatórios técnicos, manuais e documentação oriunda de palestras e simpósios realizados. Terminada a pesquisa teórica, o desenvolvimento se dará por experimentos na tentativa de executar um *software* capaz de harmonizar a emissão eletromagnética provinda de uma placa de vídeo interna de computador ligada a um monitor por um cabo VGA comum. Em teoria, com um aparelho de rádio de ondas curtas (AM), ao executar o *software*, será possível ouvir uma música gerada pela emissão eletromagnética do cabo ligado ao monitor.

Por fim, a conclusão do trabalho sobre o desenvolvimento do projeto sugerido apontando as falhas de segurança e comprovando se os objetivos foram alcançados.

2 A POLÍTICA DA INFORMAÇÃO NAS EMPRESAS

Tradicionalmente, desde a microempresa até a grande organização, é comum concentrar a atenção na segurança patrimonial visando proteger os bens materiais e restringir o acesso de estranhos nas dependências, evitando transtornos e possível prejuízo financeiro em caso de incidentes. Com a revolução digital das últimas décadas, o computador passou a ser ferramenta essencial para o processamento de dados, envio de mensagens e arquivos, digitalização de documentos, comunicação entre máquinas e diversas outras funções que agilizam processos dos quais levariam mais tempo se operados manualmente. Devido ao volume crescente de tráfego de dados circulando pelas redes de computadores, surgiu a preocupação de proteger não somente o patrimônio físico, mas também a informação na qual é transmitida, recebida e guardada através dessas redes.

Este capítulo, esquematizado de forma resumida na figura 1, aborda a realidade pela qual as companhias lidam com o acesso físico e armazenam a informação apontando as consequências de roubo, interceptação, perda de informações e quais ferramentas empregadas para manter o sistema protegido.

Figura 1 - Ilustração sobre os elementos da Segurança da Informação.
Fonte: Caruso, 2006.

2.1 Segurança da Informação

Os sistemas computacionais são a tecnologia que mais progrediu na história em um espaço reduzido de tempo, explica Tanembaum (2003). Desde meados do Século XX, a indústria da informática evolui e abrange as mais diversas áreas em poucas décadas de sua existência. O computador deixou de ser exclusividade dos centros de pesquisas e expandiu para universidades, empresas, hospitais, indústrias, bancos, ocupando funções limitadas à capacidade do ser humano. Sua abrangência alastrou ainda mais quando se fundiu com a área de comunicações ampliando o conceito de redes, no qual dois ou mais computadores são interconectados para a troca de informação e compartilhamento de periféricos, como a impressora e dispositivos de armazenamento.

A rede de computadores, comenta Tanembaum (2003), agilizou múltiplos processos morosos dentro das empresas conectando redes externas com a tecnologia procedente de cabos, fibras ópticas, antenas e satélites. Dessa forma, as mais diversificadas instituições adotaram o conceito de redes para esse fim. E a popularização da *Internet*, junto à tecnologia móvel, conectam infinidades de equipamentos simultaneamente e em qualquer lugar habitável do planeta. Porém, após o advento do primeiro vírus no final da década de 1980 (BRAIN 2011), o qual infectou inúmeros computadores pelo mundo e propagou-se por diversas redes, inclusive a BBS (*Bulletin Board System*), precursora da *Internet* popular, a segurança de dados e da informação iniciou um novo patamar na indústria computacional.

2.1.1 A informação como um ativo

Conforme explica Caruso (2006), a informação passou a ser de suma importância nas empresas e órgãos governamentais ocasionando total dependência da mesma. Seja ela em papéis, microfilmes ou digitalizada, a informação aliada à informática nas organizações atuais é proporcional à vulnerabilidade que ficam expostas a crimes e fraudes virtuais. Muitos desses crimes não são divulgados para manter a integridade da companhia, presumindo-se que o índice seja ainda maior do anunciado pelas estatísticas.

Tanembaum (2003) menciona fatos de como a informação passou a ser vital nos dias atuais na hipótese de destruição, roubo, fraude ou desastre sério no processamento de dados de uma organização causando impacto tal que levaria ao fechamento de suas portas

em mais da metade dos casos ocorridos. Mesmo um colapso no fluxo de informação, poderia fazer com que algumas empresas sobrevivessem apenas alguns dias. O valor da informação, relacionado ao produto ou serviço, é mais fundamental em algumas companhias do que o próprio produto ou serviço em si, da mesma forma que os bancos modernos não trabalham somente com dinheiro, mas com informação financeira relacionada com valores seus e de seus clientes. O banco de dados do registro de clientes de uma empresa tem um valor inestimável para ela e também aos seus concorrentes. Se houver uma quebra de sigilo e essas informações vierem a público, sua credibilidade cairá a ponto de poder decretar falência.

A grande falha em algumas companhias, segundo Atheniense (2012), é confiar cegamente em ativos físicos e financeiros (papéis) e não se atentar aos ativos de informação que possuem. É preciso repensar sobre a importância primordial que a segurança da informação chegou às organizações. Sua implementação deve ser bem estudada, avaliados diversos fatores de integridade e ser constantemente monitorada e atualizada, pois seu fluxo é sempre dinâmico e está em constante movimentação. O investimento em políticas sérias de segurança é essencial nos dias atuais apontando a tendência das empresas de até médio porte em contratar serviços especializados em prover a segurança da informação interna, enquanto que, as grandes corporações, preferem setores dedicados unicamente para essa prioridade. E a manipulação da informação (CARUSO, 2006), antes exclusividade do setor dos profissionais da área da informática[1], passou a ser gerenciada também por profissionais de outras áreas, devido à abrangência dos computadores em praticamente todos os demais setores da empresa e, consequentemente, racionou a propriedade dos ativos da informação. Assim, cada indivíduo dentro de uma empresa é responsável por cuidar da informação, eliminado o privilégio do setor de informática. As pessoas envolvidas no processo de manipulação da informação e as ferramentas lógicas existentes passam a ser incluídas na política de segurança da empresa.

2.1.2 Política de segurança

Políticas globais, apoiadas pela direção da organização, definem a responsabilidade de cada grau da hierarquia e cada grau de delegação de autoridade mostrada da forma mais

[1] Setor ou sala de informática era denominado CPD - Centro de Processamento de Dados.

clara possível (CARUSO, 2006). A política de segurança ideal é singular para cada empresa. Não há uma receita pronta que dê certo para todos os casos. Cada empresa deve moldar sua base de acordo com suas particularidades traçando um eixo com regras básicas e fazendo com que outros setores atrelados estipulem regras individuais mais detalhadas. Dentro dessa política deve haver soluções imediatas para recuperar informações evitando a inoperabilidade em caso de dano parcial ou total da capacidade de processamento. Todas as pessoas, direta ou indiretamente ligadas à organização, devem estar envolvidas, pois a segurança é uma questão de postura administrativa.

Stallings (2008) indica recomendações de segurança regidas por órgãos internacionais como a X.800 da ITU-T[2] e a RFC 2828 da IETF[3], definindo serviços de segurança que praticam políticas ou diretrizes e são exercidos por mecanismos de segurança. Esses serviços, em muitas literaturas, são chamados de 'pilares da segurança da informação', divididos em cinco categorias:

a) Autenticação: é a garantia que o emissor ou a origem dos dados recebidos é realmente de quem afirma ser ou mesmo que a comunicação seja autêntica;

b) Controle de acesso: capacidade para limitar e controlar o acesso a sistemas e aplicações através de identificação prévia;

c) Confidencialidade de dados: garante que a informação transmitida está protegida de interceptações e é acessível apenas para pessoas autorizadas;

d) Integridade de dados: determina que a informação transmitida não foi corrompida ou violada e chegou ao seu destino em perfeita exatidão dos bits de origem, conferidos por mecanismos de verificação (como exemplos a função *hash*, o SHA e o MD5[4]);

e) Disponibilidade: um sistema estará sempre disponível oferecendo serviços relativos ao projeto do sistema à medida que são requeridos por usuários autorizados.

Para Caruso (2006), deve haver equilíbrio entre ignorar e exagerar no tratamento da segurança de informação e não comprometer o investimento financeiro aplicado, ou seja, não criar normas simples demais que possam ser burladas e nem demasiadamente rígidas

---

[2] ITU-T: *International Telecommunication Union - Telecommunication Standardization Sector*: agência amparada pelas Nações Unidas desenvolvedora de padrões relacionados à telecomunicação.

[3] IEFT: *International Engineering Task Force*: comunidade internacional aberta formada por profissionais e empresas de *Internet* responsável pelas RFC (*Request for Comments*) - recomendações às questões ligadas ao uso da *Internet*.

[4] A função *hash* é um procedimento criptográfico no qual a informação é transmitida e gera um resumo de tamanho único, independente do tamanho da origem, confirmando sua integridade. Os mais conhecidos são o SHA (*secure hash algorithm*), regido pela RFC 3174 e o MD5 (*message digest algorithm*), regido pela RFC 1321.

no qual os próprios usuários cometam falhas, visto que, é impossível obter segurança absoluta. Os padrões culturais para adoção de políticas de segurança encontram resistência das pessoas no inicio, mas todos devem tomar consciência de sua importância para a empresa e seus funcionários. Praticamente, não há uma fórmula que irá servir para todas as organizações, visto que, cada uma tem sua particularidade, mas existem conceitos básicos como: criar um sistema em que a inviolabilidade dos ativos de informação seja assegurada e também a distribuição das funções individuais do usuário e dos departamentos; garantir a correta utilização do acervo de informação da qual se trata a informação e a segurança e ter em mente que, a análise do risco econômico para a segurança, tem o objetivo de instalar medidas seguras existentes em determinado ambiente, considerando três preocupações básicas: evitar a ocorrência, detectar ou combater os danos e minimizar a avaria restituindo o original o mais rápido possível.

Caruso (2006) ainda sugere uma política apoiada em um tripé composto por:

a) Redução da probabilidade de ocorrência: a prevenção de eventuais riscos antes que aconteçam será menos prejudicial do que a restauração de danos causados pela falta de segurança. Aplicam-se, nesse caso, as normas estabelecidas;

b) Redução de danos causados por ocorrências: reduzir o quanto possível caso haja uma ocorrência danosa à segurança. Aplicam-se normas e procedimentos determinados;

c) Recuperação de danos provocados por ocorrências: tomar medidas imediatas para recuperar os danos provocados pela ocorrência o quanto antes.

Os principais requisitos que governam o direito de acesso são as práticas de auditoria, a proteção de ativos e a legislação interna, informa Caruso (2006). Mesmo grandes escalões da empresa como diretores, sócios e proprietários necessitam de critérios e o administrador deve relacionar o controle de acesso em função da posição ocupada pela pessoa e não em função da pessoa. Dessa forma, será definido o acesso relacionado à posição ou cargo, pois se a pessoa se desligar ou mudar de posição na empresa, não será necessário criar uma nova política para o novo ocupante.

2.1.3 Portabilidade da informação

Um fato que preocupa os administradores de sistemas, devido à popularização mundial da informática e, por conseguinte, a *Internet*, explica Atheniense (2012), é o

compartilhamento e a troca de informação em rede pelos mais diferentes ramos e lugares. Isso aumentou consideravelmente o risco da segurança da informação nas organizações, uma vez que mais pessoas obtém conhecimento em informática e acesso a dados, fazendo com que a informação seja centralizada. Em uma companhia, qualquer pessoa com uma noção técnica avançada, além de ter acesso a informações confidenciais, pode vir a lucrar com elas. Além disso, a portabilidade e a distribuição da informação ficam a cada dia mais facilitadas com mídias portáteis e sua capacidade de armazenamento. Com o avanço da tecnologia, reduzindo medidas e aumentando velocidade, volumes de informação são armazenados em espaços cada vez mais restritos. Equipamentos e mídias passam a ser mais leves e portáteis, permitindo operar em espaços menores e transportados com mais facilidade. Uma informação confidencial pode rapidamente ser transportada em um dispositivo portátil (telefone móvel, câmera digital, discos ou cartões de armazenamento), transmitida pelo ar (via *bluetooth* ou rede sem fio) ou enviada pela *internet* por um *modem* de telefone móvel. Do mesmo modo, alguém pode executar programas que podem disseminar vírus e *softwares* espiões, comprometendo o sistema da companhia.

Outro fator agravante, segundo Mitnick (2003), é a falta da cultura de segurança da informação nas empresas. Com o uso da engenharia social[5], por exemplo, um indivíduo consegue persuadir um vigia, ter o acesso físico nas dependências da empresa, emprestar ou roubar uma senha e obter o acesso lógico ao sistema. Essa forma de intrusão é mais perigosa por ser invisível e de difícil detecção, caso não seja empregadas ferramentas apropriadas de monitoramento. Além disso, o descarte inadequado de material com registro de informação, como papéis impressos, discos ópticos, fitas e discos rígidos[6] é praticamente ignorado. Se não aplicados procedimentos corretos de descarte ou troca de equipamentos, esse material poderá ser retido por criminosos com o propósito de recuperar a informação supostamente apagada.

Um ambiente operacional (CARUSO, 2006) é formado pela combinação de equipamentos, *softwares*, linhas de comunicação, pessoas e procedimentos dentro de um sistema de comunicação de dados - porta de entrada para os usuários conseguirem acesso ao ambiente de informação. E é justamente nesse acesso, no qual a informação trafega e é

[5] Engenharia social é uma prática de abordagem às pessoas, explorando sua distração e ingenuidade, para obter informações, senhas, acessos e documentos restritos (MITNICK, 2003).
[6] O disco rígido permite recuperar dados mesmo depois de apagados ou após sua formatação.

armazenada, em que há o maior fator de risco, incluindo ataques ao sistema, roubo de informação e destruição de dados. Portanto, as possibilidades de violação do sistema de uma organização aumentam se não adotadas e cumpridas as políticas de seguranças física e lógica estabelecidas, através de controle de acesso combinados com ferramentas de análise e auditorias periódicas, a informação e os ativos da organização ficarão comprometidos.

2.2 Segurança Física

Em um levantamento de auditoria em diversas empresas, descreve Caruso (2006), foram constatadas inúmeras irregularidades nas instalações da sala de informática. A começar da própria construção em locais predispostos a incêndio e campos magnéticos, equipamentos inadequados de combate ao fogo, instalações elétricas precárias, incidência direta de raios solares, climatização deficiente ou sobressalente. Sistemas não automatizados de controle de acesso físico, energia elétrica alternativa com baterias e geradores defeituosos e em condições perigosas, falta de treinamento de profissionais em caso de emergências e muitos outros itens.

Acontecimentos históricos ocorridos em países mais desenvolvidos (CARUSO, 2006), fizeram com que a preocupação da segurança física nas salas de informática aumentasse devido a vários atentados. Em virtude disso, esses países se especializaram no assunto e amadureceram o conceito de segurança construindo instalações dotadas de normas de nível militar para proteção do setor. Com isso, foi aprendido que, as instalações das salas precisam ser exclusivas e não compartilhadas com outro setor. Devem ficar afastadas de locais perigosos, como empresas químicas, antenas de transmissão, estações de energia elétrica, vibrações de alto impacto, entre outros fatores ambientais. O piso deve ser elevado para facilitar a passagem de cabos, tetos e paredes em que não passem encanamentos, portas resistentes a fogo e de fechamento automático, chuveiros automáticos de incêndio, extintores apropriados à ocorrência. Possuir iluminação e acabamentos adequados, sinalização de fácil visualização e compreensão, materiais em geral e móveis incombustíveis e muitas outras lições aprendidas com o decorrer dos fatos.

No conceito de Stallings (2008), o acesso físico ao sistema deve ser eficiente. Ele classifica três tipos de intruso: *mascarado*: indivíduo ligado ou não à empresa, sem autorização de uso em computadores, mas adentra nos controles de acesso explorando uma

conta de usuário legítima; *infrator*: usuário autorizado e limitado a utilizar o sistema, certos *softwares* e recursos, mas, mesmo assim, explora áreas proibidas fazendo o uso indevido dos privilégios que recebeu; *clandestino*: indivíduo com posse de autoridade de supervisor do sistema com o intuito de fugir do controle de acesso e esconder provas de auditoria.

Caruso (2006) propõe a instalação de obstáculos físicos intimidadores para controle de acesso físico desde a entrada ao recinto (guarita, recepção e estacionamento) até locomoção interna na empresa entre os setores: sistema de alarme com câmeras de vídeo ativas e gravação ininterrupta; cerca-elétrica; delimitação de zonas de segurança e níveis de riscos sinalizados e explicativos, além de indicativos visuais e sonoros para as áreas de fuga de emergências; treinamento preventivo pessoal de combate ao incêndio, resgate, tratamento e locomoção das pessoas em emergências; armazenamento de documentos, cópias de segurança (becapes) e mídias em cofre contra fogo e magnetismo situado em sala altamente segura com câmeras e acesso restrito; transporte cauteloso de mídias sensíveis a impactos mecânicos, térmicos e eletromagnéticos; temperatura, poeira e umidade controladas; proteção contra incêndio e instalação elétrica e iluminação adequadas.

O acesso físico de um ativo tem menos riscos de certa forma, comparado ao acesso lógico, esclarece Atheniense (2012). Porém, seu controle é mais difícil e depende totalmente da intervenção humana. Pelo fato de muitas organizações ficarem atreladas ao ambiente de informação, essencialmente, a integridade dos dados nesse ambiente, deve estar seguro de quaisquer ameaças e possuir um plano de recuperação dinâmico para conservação dos ativos. Essa estratégia é chamada de plano de contingência. Somados aos conceitos de segurança física e plano de contingência, há ainda o conceito de preservação e recuperação de informação e seus ativos, como cópia de segurança e outros procedimentos, nos quais se tornam imprescindíveis para sobrevivência da organização no caso de acidentes. Por fim, manter uma rotina de auditoria e manutenção constantes nos equipamentos de combate ao incêndio e segurança, além de toda estrutura patrimonial da organização.

2.3 Segurança Lógica

O termo ‘segurança de rede’ não é bem colocado, segundo Stallings (2008), já que as organizações, universidades e governo interconectam suas redes internas com um conjunto de outras redes interconectadas, assim, o correto seria dizer ‘segurança de inter-rede’.

Independente da definição - comenta Atheniense (2012), o mercado oferece diversos mecanismos para o controle de acesso lógico ao sistema de computadores da rede, no qual condicionam o usuário a explorar somente a área e os dados autorizados a ele. A senha digitada por uma sequência de caracteres memorizados pelo usuário é um dos mecanismos mais antigos e empregados nas empresas. Porém, é ultrapassado e passível de falhas, uma vez que existe a possibilidade de a senha ser extraviada ou mesmo esquecida, gastando-se tempo desnecessário para sua recuperação.

Com a evolução dos equipamentos de segurança, explica Caruso (2006), a tendência segue a utilizar características físicas do usuário, como na biometria, o qual os dedos, mãos, face, olhos, voz, entre outros são utilizados e vem gradativamente substituindo a tradicional senha digitada. *Softwares* com chaves digitais de acesso são outro tipo de tecnologia empregada, no qual o usuário recebe uma chave pública associada a uma senha capaz de autenticá-lo aos recursos respectivamente autorizados a esse usuário, sendo unicamente responsável por todas as ações que cometer. O ingresso a esses recursos também pode ser controlado por listas de acesso dispostas em uma tabela que liga o usuário ao tipo e ao recurso da operação do qual for determinada sua permissão. Essas listas podem ser combinadas às chaves de acesso citadas. Após ser aprovado pelo controle de acesso inicial, o usuário, de acordo com sua função, ficará limitado a operar certos recursos como leitura, gravação, alteração, exclusão, eliminação de arquivos e execução de *softwares*. Esta característica tem um fator hierárquico da qual terá mais ou menos privilégios de acordo com a função determinada ao usuário.

Com o conhecimento das ferramentas disponíveis, o administrador de sistemas, segundo Caruso (2006), terá que definir o inventário de usuários e relacioná-los aos recursos que terão acesso. Em princípio, deve ser criado um banco de dados dos usuários incluindo seu código de identificação e/ou chave acesso, domínios pertencentes e outros dados pessoais. Depois, definir os grupos divididos segundo a política estabelecida pela organização, listando os recursos existentes, as responsabilidades e finalmente estabelecer os perfis (atual e desejado).

Assim, o acesso ao sistema deve incluir: a proteção de subsistemas; identificação; controle de senhas e de submissão de tarefas; restrições de data e hora (evitando o uso não autorizado fora do expediente de trabalho); controle de submissão automática de tarefas; controle sobre rotinas internas de submissão de tarefas pelo sistema e suporte para

monitores de acesso de outros fornecedores. Já o acesso de usuários aos recursos é dividido em tipos de recursos protegidos: proteção de arquivos, programas e comandos, interfaces com *softwares* gerenciados de banco de dados e transações, dispositivos-padrão de segurança e interfaces com outros *softwares*.

Há recursos para auditagem e controle que devem relacionar as facilidades do pacote de segurança à sua estrutura, descreve Caruso (2006). Além disso, a adoção da criptografia[7] é essencial para dificultar a interpretação dos dados, sejam eles acessados pela rede interna ou trafegados externamente, como por exemplo, na transmissão de dados por antenas ou mesmo pela *internet*. Além desse procedimento, utilizar formas para complementar a segurança como: definir o tamanho das chaves digitais e trocá-las com frequência, adotar rotas alternativas, criptografar, compactar e autenticar mensagens, transmitir em blocos e utilizar cifragem também em situações diversas. As chaves digitais públicas fortalecem a segurança, sendo um modo eficaz no qual um emissor gera uma chave pública junto à mensagem, passível de ser decifrada por quem possuir a chave particular gerada, nesse caso o receptor.

2.3.1 Vulnerabilidades em redes externas

Para Atheniense (2012), a *Internet* abriu as portas da comunicação em massa e expandiu o conceito de redes, antes restrito apenas às companhias. Agora, a grande rede mundial liga datacenters a computadores domésticos e dispositivos móveis. Essa facilidade também trouxe grande impacto de risco à informação nas companhias, necessitando repensar a política de segurança e estreitar cada vez mais o acesso. Stallings (2008) comenta que antes mesmo da abertura mundial de mercado da *Internet*, início da década de 1990, vários órgãos internacionais[8] alertavam sobre a segurança *online* identificando precauções contra vulnerabilidades, como a necessidade de proteção do tráfego contra acessos não autorizados e monitoração na infraestrutura da rede utilizando mecanismos de autenticação e criptografia. Um dos maiores vilões, provavelmente, seja o correio eletrônico que, além de

[7] Criptografia, segundo Kurose e Ross (2006), é uma técnica que disfarça os dados transmitidos por seu destinatário, devidamente habilitado, e recupere os dados originais com base na informação recebida, evitando algum intruso decifrar certo dado interceptado.

[8] O IAB (*Internet Architecture Board*) emitiu o relatório '*Security in the internet architecture*' (RFC 1636) e o CERT (*Computer Emergency Response Team*) divulgou estatísticas de vulnerabilidade da *Internet* perante ataques a sistemas como negação de serviço, falsificação de IP, farejamento de pacotes, entre outros.

disseminar vírus, aumenta o tráfego da rede com propaganda eletrônica. A transferência de arquivos na rede sem controle também aumenta o tráfego exigindo muito mais das máquinas e criando indesejáveis gargalos. Além de websites que podem conter códigos maliciosos e abrir brechas para invasões no sistema.

Outra facilidade da tecnologia de redes, apresenta Tanenbaum (2003), é o acesso remoto no qual o usuário autorizado consegue acessar a rede interna da companhia em praticamente qualquer local em que haja linha telefônica ou *internet* disponível, como se estivesse pessoalmente nas dependências da empresa. Entretanto, deixa brechas para possíveis invasões. O interesse das pessoas com esse intuito varia desde a curiosidade de bisbilhotar arquivos e mensagens, roubar ou manipular dados e derrubar o sistema (por exemplo, um ex-funcionário se vingando por sua demissão). Pode ainda espionar estratégias do concorrente, desviar valores para uma conta bancária pessoal ou mesmo testar a fragilidade da segurança, podendo deixar um assinatura em algum local do sistema, destruir dados ou, mais racionalmente, alertar sobre a falha para a empresa e lucrar com isso.

Enfim, conclui Caruso (2006), o método padrão a ser empregado, desde a implementação das políticas, deverá ser o de adotar uma solução simplificada, como a filosofia básica sobre segurança de redes, no qual utiliza o menor privilégio possível inicialmente para todos, ou seja, o que não é explicitamente permitido será proibido. A peça chave é restringir o acesso da rede interno ao externo e vice-versa. Para isso, além do amadurecimento da política e cultura de segurança, deve ser instalados equipamentos e *softwares* para filtrar esses acessos. O primordial é que apresente *firewalls* (barreiras de entrada e saída de dados), antispams (bloqueio de mensagens com propaganda não solicitada), antivírus (eliminação de pragas virtuais) e monitores de rede (analisam se há algum estouro de memória ou uso excessivo de algum recurso provindo de uma suposta invasão no sistema). Além de sempre atualizar os sistemas operacionais, *softwares* e drives, consultar relatórios (*logs*), programar disparadores de alerta por mensagens eletrônicas e via telefone móvel e auditar, com certa frequência, o sistema completo como um todo.

3 SEGURANÇA POR MEIO DE BLINDAGEM

Com a crescente demanda e popularização de equipamentos eletroeletrônicos nas cidades, empresas e residências, os fabricantes viram a necessidade de revisar seus projetos para que um equipamento não entre em conflito ou interfira na função do outro. Um dos métodos mais eficientes para evitar esses problemas é reduzir o campo magnético emitido por esses equipamentos por meio de blindagem de cabos e gabinetes. Caso seja inviável, deve ser feito ajustes nos circuitos eletroeletrônicos para que a emissão seja ao menos dentro de uma faixa de frequência que interfira em uma gama menor de equipamentos.

O assunto será relatado neste capítulo visando não só as interferências causadas pela radiação eletromagnética, mas também o vazamento de informação passível de captação à distância ultrapassando as barreiras físicas e lógicas conhecidas e toda a infraestrutura de segurança adotada pela organização.

3.1 A emissão de ondas eletromagnéticas - EMR

O ser humano não inventou as ondas eletromagnéticas, mas aprendeu a utilizá-las (BALAN, 1999). Com o estudo da Física, esclarece Tanenbaum (2003), descobriu-se que essas ondas são compostas por campos elétricos e magnéticos (figura 2), geradas pela movimentação dos elétrons e dissipadas pelo ar ou no vácuo sendo propagadas à velocidade da luz em 300.000 km/s (quilômetros por segundo).

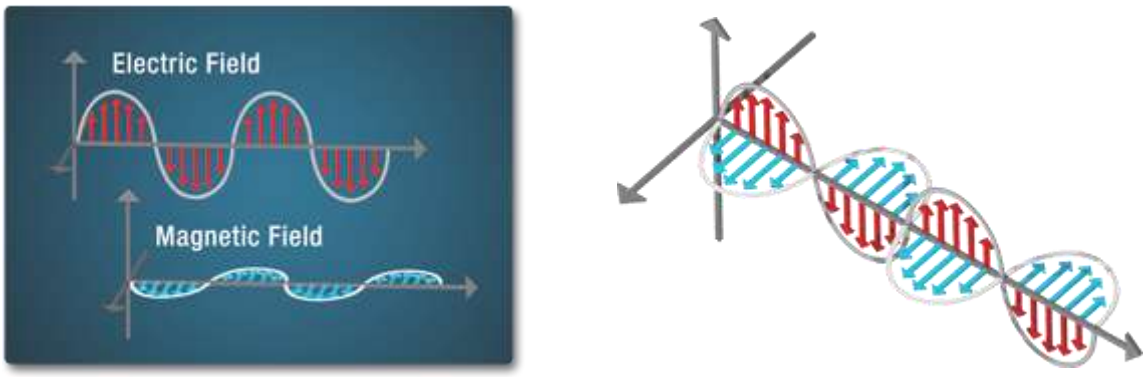


Figura 2 - Gráficos representando o campo elétrico (*electric field*) perpendicular ao campo magnético (*magnetic field*) formando a onda eletromagnética (à direita). Fonte: NASA (BUTCHER, 2010).

A dissipação de uma onda sofre inúmeras variações dependendo de como foi originada (OMOTE, 1982). Basicamente, essas variações são classificadas pela sua forma (senoidal, quadrada, dente de serra ou triangular); intensidade (medida pela amplitude (a),

simbolizada no eixo Y do gráfico da figura 3); polarização (polarizada com um só vetor ou não polarizada com vários vetores diferentes); período (medido por segundos (s) e simbolizado no eixo X do gráfico da figura 3); polaridade (positiva [+], neutra [0] ou negativa [-]) e pelo seu comprimento (distância da formação até o término da onda, simbolizado por λ (lambda) no gráfico da figura 3).

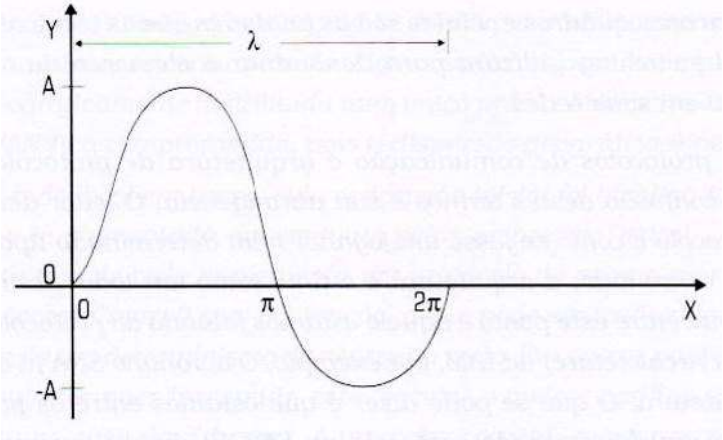


Figura 3 - Gráfico representando a forma de uma onda senoidal.
Fonte: Dantas, 2002.

No campo da Física, segundo Omote (1982), a onda é entendida como uma perturbação (pulso) que se propaga no espaço distanciando-se de seu ponto de origem. Ela dissipa energia sem dissipar ou consumir a matéria. Um exemplo clássico para explicar estes fatos parte de quando se joga uma pedra em uma lagoa com a água em repouso (figura 4). É possível visualizar as ondas se formando ao redor do ponto em que a pedra tocou na água e assim, comprovar o efeito da propagação afastando-se do ponto de origem, sem consumir nenhum dos materiais (pedra e água), apesar da manifestação de energia dissipada na água.

Figura 4 - Fotografia representando o efeito da perturbação na água gerando ondas.
Fonte: NASA (BUTCHER, 2010).

A quantidade de oscilações ou ciclos de onda eletromagnética contabilizadas no período de um segundo (s) é chamada de frequência e sua unidade de medida é o Hertz (Hz). Frequência e período, conforme apresentado nas expressões em [1], são grandezas inversamente proporcionais:

$$\textit{frequência (Hz)} = \frac{1}{\textit{período}} \qquad \textit{período (s)} = \frac{1}{\textit{frequência}} \qquad [1]$$

Deste modo, ciclos ilimitados podem ocorrer no mesmo período de um segundo fazendo elevar a frequência e seu número de Hertz, como exemplificado na figura 5. Porém, explica Tanenbaum (2003), com o aumento de frequência, as ondas ficam cada vez mais estreitas e próximas umas das outras a ponto de apenas uma fração delas poder ser vista pelo olho humano e outra fração ser ouvida.

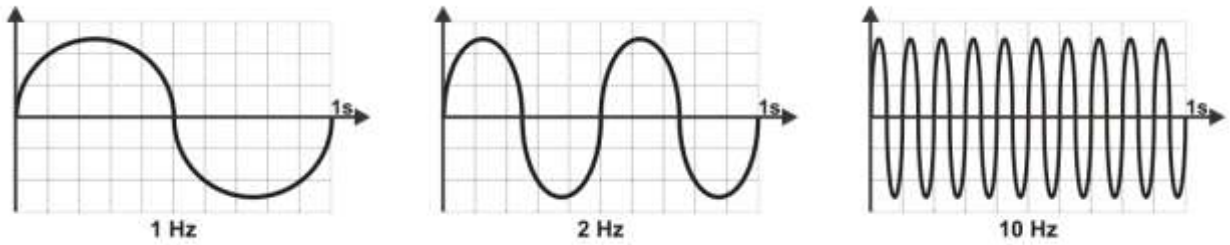


Figura 5 - Gráficos representando ciclos de frequência de onda no mesmo período de um segundo.
Fonte: própria.

A ilustração da figura 6 mostra o comportamento das ondas à medida que sua frequência se eleva. No primeiro índice (comprimento de onda), há uma régua com escalas em metros a ser comparada ao segundo índice (dimensão do comprimento de onda) que exibe exemplos dessas escalas. Um campo de futebol tem seu comprimento aproximado de cem metros (10^2 m), uma bola de beisebol: dez centímetros de diâmetro (10^{-1} m), um ponto simples: um milímetro (10^{-3} m), uma bactéria: um micrometro ou mícron (10^{-6} m) e a molécula de água: um décimo de nanômetro (10^{-10} m). Com base nesses extremos, é possível fazer a comparação com os próximos índices.

Frequências mais baixas utilizadas pelas estações de rádio, televisão e similares (radioamador, aviação, polícia, bombeiros) viajam na ordem de centenas de metros até vários quilômetros (BUTCHER, 2010). Nos índices de origem e frequência (figura 6) é ilustrada a estação de rádio AM que compreende a faixa de 520 a 1610 kHz (quilo-hertz ou 10^3 Hertz) e tem alcance de quilômetros (10^3 metros) chegando no caso a atravessar países

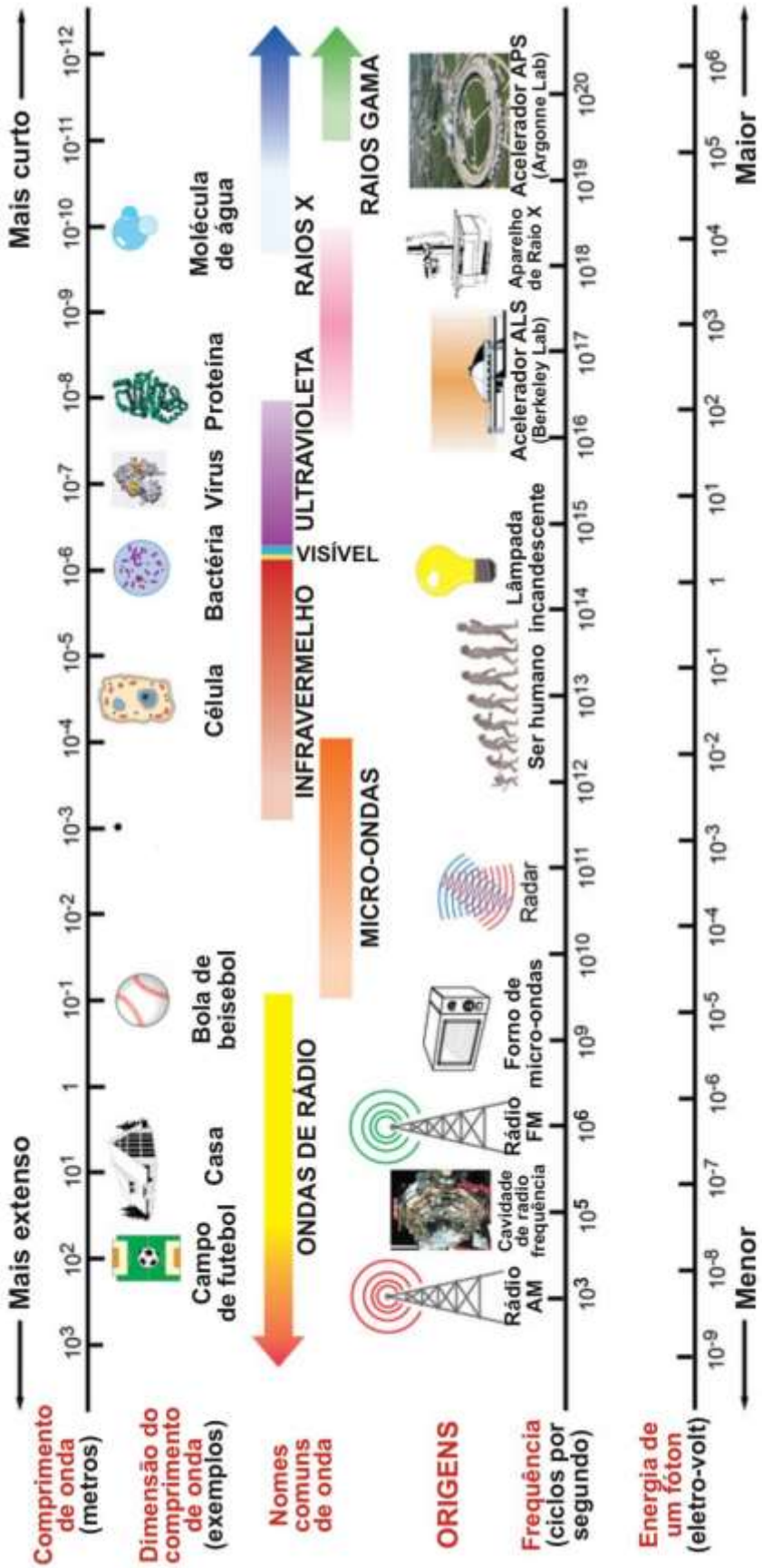


Figura 6 - Ilustração sobre a dimensão do espectro eletromagnético em elementos da Física.
Fonte: Advanced Photon Source (THE ELECTROMAGNETIC SPECTRUM, 2011).
(adaptado - tradução livre).

dependendo de obstáculos e fatores climáticos em sua rota. Da mesma forma, a estação de rádio FM, na faixa de 88 a 108 MHz (mega-hertz ou 10^6 Hertz) e certas estações locais de televisão (VHF e UHF) alcançam alguns quilômetros ao redor da estação transmissora. A seguir, a escala de frequência passa a se estreitar na ordem acima de três bilhões de ciclos por segundo e cada ciclo medindo menos de um milímetro (10^{-3} metro) de comprimento.

A faixa de micro-ondas, de 3 a 30 GHz (giga-hertz ou 10^9 Hz), é empregada na transmissão via satélite, telefonia celular e radares, contudo, cada tecnologia tem sua dinâmica de antenas distintas (BUTCHER, 2010). Na transmissão via satélite, antenas de grandes dimensões são posicionadas precisamente para o satélite correspondente que irá retransmitir o sinal a uma região específica do planeta. Essa transmissão normalmente é feita por emissoras de televisão, estações meteorológicas e órgãos militares. Para a recepção do sinal, as antenas são menores, mas devem estar apontadas com precisão ao satélite apropriado. Na telefonia celular e *internet* móvel as antenas seguem o sistema de MTSO (central de comutação de telefonia móvel) onde a transmissão e recepção do sinal são roteadas por diversas antenas de acordo com a locomoção do aparelho de celular.

Já os radares são baseados na ecolocação, característica de animais como o morcego, a baleia e o golfinho. A antena desses equipamentos transmite um sinal curto e potente (BUTCHER, 2010) e, logo em seguida, a mesma antena capta o retorno do sinal transmitido para calcular a distância e velocidade de outros objetos ao seu redor. Sonares de submarinos funcionam de forma parecida com sinais de frequência mais baixos devido à dificuldade de propagação na água. O forno de micro-ondas (apesar de não pertencer à área de comunicações, foi descoberto por meio dela) emite ondas que agitam as moléculas de água dos alimentos elevando sua temperatura e assim cozinhando-os. A próxima escala de frequência chega a trezentos trilhões de ciclos por segundo.

A radiação infravermelha (IR), de 300 GHz a 300 THz (tera-hertz ou 10^{12} Hz), é a qual o corpo humano emite e é visível apenas para alguns animais como a cobra. Possui aplicação em câmeras de vigilância (visão noturna), sensores, alarmes, controles remotos, fornos, estufas, equipamentos médicos e militares. Na figura 7 é demonstrada a utilização do mapa térmico em um cachorro onde é possível, através da radiação infravermelha, verificar a temperatura nos diferentes pontos do corpo. Omote (1982) explica que, quando a radiação infravermelha chega ao seu limite máximo no espectro eletromagnético, inicia-se a radiação visível ao olho humano (luz) na faixa de frequência entre 400 e 750 THz.

Figura 7 - Ilustração captada por uma câmera de radiação infravermelha exibindo o mapa térmico de um cachorro. Os pontos mais escuros (violeta) são os mais frios (70° Fahrenheit ou 21° Celsius), enquanto que os pontos mais claros (próximo do vermelho) são os que estão mais quentes (94° Fahrenheit ou 34° Celsius). Fonte: NASA (BUTCHER, 2010).

A luz, como conhecemos, é essencial para a visibilidade das pessoas e para o efeito de fotossíntese nas plantas. Seu espectro é composto de sete cores (arco-íris), do vermelho ao violeta, e cada cor tem sua faixa de frequência específica, como apresentado na tabela 1.

Tabela 1 - Característica do espectro da luz branca visível aos seres humanos (valores aproximados).

COR	COMPRIMENTO DE ONDA (nanômetros)	FREQUÊNCIA (THz)
VERMELHO	625 - 740	430 - 480
LARANJA	590 - 625	480 - 510
AMARELO	565 - 590	510 - 530
VERDE	500 - 565	530 - 600
CIANO	485 - 500	600 - 620
AZUL	440 - 485	620 - 680
VIOLETA	380 - 440	680 - 750

Fonte: Hewitt, 2002.

A soma destas cores resulta na luz branca irradiada pelo sol. Um corpo iluminado terá determinada cor conforme sua capacidade de absorver e refletir as radiações incidentes. Por exemplo, se um corpo incide a luz branca do sol e aparece verde, então se diz que esse corpo reflete o verde e absorve as outras cores.

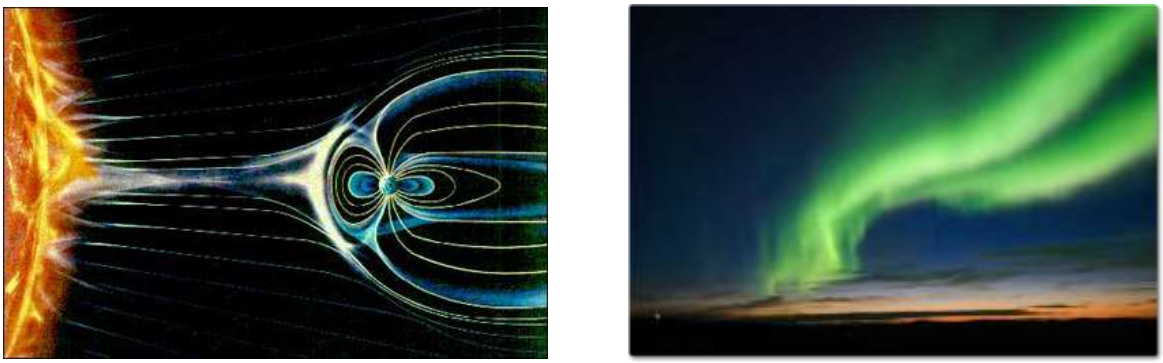


Figura 8 - A Ilustração à esquerda mostra explosões solares que bombardeiam o campo magnético da Terra com radiação ultravioleta e gases causando o fenômeno aurora boreal (fotografia à direita). Fonte: NASA (BUTCHER, 2010).

Na extremidade posterior à cor violeta, segue a faixa da radiação ultravioleta (UV) compreendida nas frequências de 750 THz a 300 PHz (peta-hertz ou 10^{15} Hz) e comprimento de onda de milésimos de milímetro, próximo ao tamanho de um vírus (10^{-7} metro).

A radiação ultravioleta só é visível por animais como a abelha e sua radiação ajuda a provocar o fenômeno aurora boreal (figura 8) em certos países. É difundida em áreas de química, biologia (bactericida, atração de insetos), medicina, indústria, segurança (identificação de notas falsificadas, análise forense), informática (apagamento de memórias eletrônicas), entretenimento (luz negra), astronomia (satélites, sondas espaciais) e em pesquisas científicas sobre fluorescência e simulação de envelhecimento de materiais.

O sol é a maior fonte de radiação eletromagnética próxima à Terra (HEWITT, 2002). Sua energia chega ao planeta composta pelas radiações: infravermelha (calor: 52%), visível (luz: 41%) e ultravioleta (7%). Apesar da porcentagem de ultravioleta ser menor, é a qual causa danos à saúde como o câncer de pele se a exposição ao sol for demasiada, porém, ela é importante para a absorção da vitamina D pelo organismo humano e para manter o clima do planeta aquecido. A radiação ultravioleta tem três categorias básicas: UVA (90%), UVB (10%) e UVC (é quase totalmente barrada na atmosfera pela camada de ozônio).

Completando as faixas do espectro eletromagnético, demonstradas na figura 6, há os raios X (10^{16} a 10^{19} Hz) e os raios gama (10^{19} a 10^{22} Hz), com o comprimento de onda menor que a molécula de água (10^{-10} m). Os raios X são amplamente usados em medicina (radiografia, tomografia, ressonância magnética e radioterapia), química, biologia, segurança (aeroportos) e indústria. Os raios gama também têm uso em medicina, química e biologia, contudo, é mais utilizado em astronomia e radiação nuclear (BUTCHER, 2010). Ambos os raios são pesquisados em laboratórios de aceleradores de partículas (quebrador de átomos) em diversos países, como os laboratórios ALS de Berkeley e o APS de Argonne, ambos dos Estados Unidos. Além da frequência de 10^{22} Hz (zeta-hertz ou ZHz) existem os raios cósmicos que, na realidade, são partículas de átomos e estão presentes em todo o universo e, inclusive, penetram na atmosfera terrestre, mas não são prejudiciais, exceto no espaço sideral onde sua intensidade é maior.

O último índice da figura 6 mostra a escala referente ao fóton, a menor partícula de luz existente, deste modo, é indivisível e nunca fica em estado de repouso (HEWITT, 2002). O fóton, simbolizado por γ (gama) na figura 9, constitui-se de campos elétricos e magnéticos, devido a certos fluxos de elétrons em um átomo, formando a onda eletromagnética

composta de energia. Essa energia é proporcional à frequência da onda, portanto, quanto maior a frequência, maior energia e impulso o fóton terá. O valor de um eletro-volt, mostrado na escala da figura 6 é exatamente a faixa de luz visível.

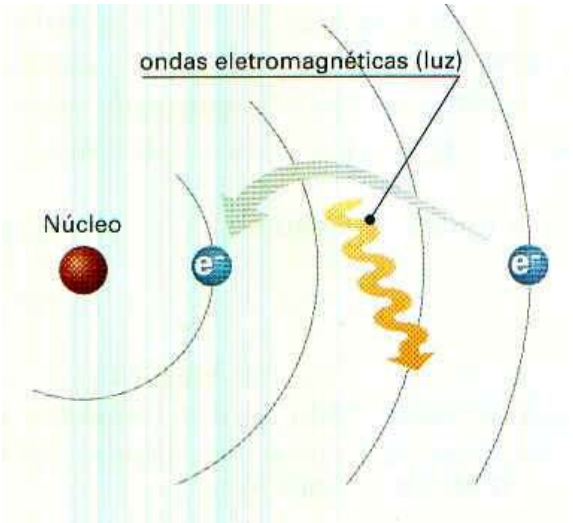


Figura 9 - Ilustração de uma onda eletromagnética (fóton) gerada pelo fluxo de elétrons em um átomo.
Fonte: Prof. Paulo César (MODELO ATÔMICO ATUAL, 2010).

3.1.1 As ondas eletromagnéticas nas telecomunicações

Existem subdivisões de faixas de frequência chamados banda e trabalham em campos definidos por padrões internacionais. As bandas mais conhecidas estão representadas na Figura 10, onde são mostradas também, as faixas de frequência dos cabos comuns em telecomunicações: o par trançado (*twisted pair*, de 10^4 a 10^8 Hz), coaxial (*coax*, de 10^5 a 10^9 Hz) e a fibra óptica (*fiber optics*, faixa de 10^{14} a 10^{15} Hz). A Tabela 2 mostra, em resumo, as aplicações comuns em telecomunicações subdivididas por faixas de frequência e banda, assim como o uso outras áreas.

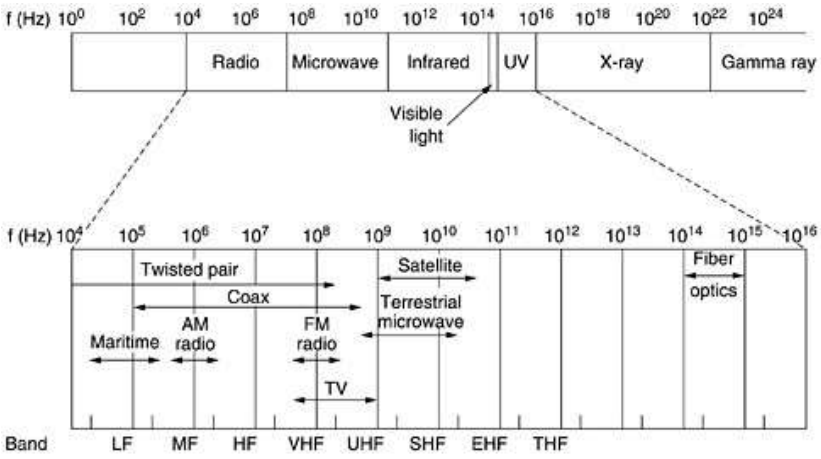


Figura 10 - Representação do espectro eletromagnético e seu uso em telecomunicação.
Fonte: Tanenbaun, 2003.

O fundamento básico da comunicação sem fios (TANENBAUM, 2003) parte do princípio que sempre haverá um transmissor, composto de uma antena ligada a um circuito eletrônico, enviando o sinal onde será captado por um receptor com estrutura semelhante ao do transmissor.

Tabela 2 - Faixas de frequência subdivididas conforme aplicações.

FREQUÊNCIA (EM HERTZ)	APLICAÇÃO	FAIXA	BANDA
20 a 20.000	Aparelhos musicais	Sons audíveis pelo ser humano	LF
20.10^3 a 30.10^3	Medicina, Militar	Ultrassom	LF
530.10^3 a 1600.10^3	Rádio AM	Rádio	MF / HF
30.10^6 a 300.10^6	TV		VHF
88.10^6 a 108.10^6	Rádio FM		
143.10^6 a 148.10^6	Radioamador		
300.10^6 a 3.10^9	TV		UHF
3.10^9 a 30.10^9	TV Satélite, Celular	Micro-ondas	SHF
300.10^9 a 300.10^{12}	Controle remoto, Medicina, Militar	Infravermelho	EHF / THF
750.10^{12} a 300.10^{15}	Medicina, Biologia	Ultravioleta	-
10^{16} a 10^{19}	Medicina, Segurança	Raio X	-
10^{19} a 10^{22}	Medicina, Militar	Raio Gama	-

Fonte: Balan, 1999.

Vários fatores irão influenciar na eficiência da transmissão e captação de sinais como o projeto de fabricação, o tamanho e localização da antena, a qualidade dos componentes eletrônicos e a potência do transmissor da estação. Compreende-se também, os obstáculos e situações meteorológicas, interferências de outras antenas ou equipamentos e a distância física entre transmissor e receptor.

3.1.2 Certificações para emissão de ondas eletromagnéticas

Todo e qualquer equipamento eletroeletrônico deve passar por inúmeros testes antes de ser comercializado. Dentre estes testes (BRASIL, 2007), está a emissão de ondas eletromagnéticas (EMR) no qual há dois fatores a ponderar: a intensidade máxima de dissipação e a faixa de frequência irradiada para que não interfira em outros equipamentos ao seu redor. Segundo o Comitê Brasileiro de Avaliação da Conformidade – CBAC[9] é

[9] O CBAC é um grupo de trabalho formado por outras associações brasileiras: ABINEE, ABIMAQ, ELETROS e ABNT/CB 26 que busca tratar o quesito da compatibilidade eletromagnética no Brasil.

necessário estabelecer um programa abrangente para adequar produtos elétricos, eletrônicos e eletroeletrônicos defronte à interferência eletromagnética, já que o país não dispõe de normas específicas sobre o assunto. Na 17ª reunião ordinária do CBAC, realizada em 2007, foram criados parâmetros nos quais o equipamento testado tende a se comportar:

a) Compatibilidade eletromagnética (EMC): capacidade do equipamento ou sistema para funcionar satisfatoriamente em seu campo de alcance sem causar perturbações intoleráveis a qualquer coisa nesse ambiente;

b) Perturbação eletromagnética: qualquer fenômeno eletromagnético que afete o desempenho de equipamentos ou sistemas ligados ou em modo de economia de energia;

c) Interferência eletromagnética (EMI): degradação do desempenho de um dispositivo ou sistema causado pela perturbação eletromagnética;

d) Emissão eletromagnética: quando o fenômeno causador da energia eletromagnética provém da fonte;

e) Imunidade à perturbação: habilidade do equipamento funcionar sem degradar seu desempenho devido à presença de uma interferência eletromagnética;

f) Requisitos de emissão de perturbações eletromagnéticas: limites estabelecidos para as perturbações emitidas pelos equipamentos, na forma conduzida ou na forma radiada, visando proteger equipamentos do ambiente contra a interferência;

g) Requisitos de imunidade a perturbações eletromagnéticas: limites estabelecidos de modo a garantir o funcionamento normal de equipamentos, quando estes são submetidos a perturbações eletromagnéticas, na forma conduzida ou radiada, com intensidade compatível com seus ambientes de operação.

Em outros países, conforme indica o CBAC (BRASIL, 2007), estas questões já estão formalizadas há algum tempo. A organização anglo-suíça International Electrotechnical Commission - IEC definiu as normalizações IEC 61000 e IEC 60601. Na Europa, está em vigor a Diretiva Europeia 89/336/EEC que trata da compatibilidade eletromagnética, sendo obrigatória desde 1992. Na América do Norte, a Federal Communications Commission - FCC, órgão regulamentador federal, determinou que todos os equipamentos emissores de radiointerferência estão sujeitos aos requisitos da FCC e devem ter uma identificação da conformidade expressa como “Declaração da conformidade” ou “Certificação”. Na Austrália, a Australian Communications Authority - ACA regulamenta os parâmetros da compatibilidade eletromagnética, além de telecomunicações e radiocomunicação. Na Nova

Zelândia, o Ministério do Comércio regulamenta compatibilidade eletromagnética e radiocomunicação e assim como na Austrália, a regulamentação é independente, porém, baseada na "Declaração da Conformidade" onde os produtos são classificados em três níveis, de acordo com o possível risco de interferência: nível 1 – baixo risco de impacto; nível 3 – alto risco de impacto; nível 2 – produtos não enquadrados em 1 e 3. As únicas regulamentações do Brasil provêm de equipamentos eletromédicos:

a) A Agência Nacional de Vigilância Sanitária - ANVISA, com as portarias do Ministério da Saúde nº 2043 de 12/12/1994, nº 155, de 27/02/97 e nº 1104, de 30/08/99; Resoluções RDC nº 32, de 29/05/07, RE nº 1746, de 25/10/2001 e 1829, de 06/11/2001;

b) O Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - INMETRO, com a portaria 86, de 03/04/06;

c) A Agência Nacional de Telecomunicações - ANATEL, sobre os equipamentos de telecomunicações com resolução nº 442 de 21/07/06 que são submetidos aos ensaios compulsórios quanto aos aspectos de compatibilidade eletromagnética.

Ainda em fase de elaboração, a Associação Brasileira de Compatibilidade Eletromagnética - ABRICEM, está criando uma norma ABNT sobre a emissão gerada em subestações de energia elétrica (ABRICEM, 2000). Há um parágrafo no decreto de lei nº 7.174, de 12 de maio de 2010, citando a compatibilidade magnética dos equipamentos e serviços de informática adquiridos pelo Poder Público (BRASIL, 2010).

Uma leitura atenta nas regulamentações citadas irá mostrar o fator humano como principal prejudicado quando há vazões de energia eletromagnéticas, seja por equipamentos que adquiriu, seja pelo ambiente em que vive carregado de diversas emanações originadas das grandes cidades e empresas, expondo risco à saúde do indivíduo (APÊNDICE D). Mas, outro fato preocupante, são os equipamentos que processam informação como: computadores, impressoras, monitores e teclados (BLACK BOX, 2012). Dependendo do ambiente ao redor dos equipamentos (SCAGLIA, 1998), as emissões geradas podem se propagar por tubos de água, barras de ferro usadas na construção de paredes e concreto, fios elétricos e telefônicos. Assim, qualquer pessoa com uma base de conhecimento em eletrônica e uma aparelhagem adequada, que vai desde um simples rádio, consegue captar essas emissões à distância, decodificar e ver os dados brutos oriundos de um monitor, saída de impressora ou mesmo digitado no teclado. Desta forma, o invasor obtém um equipamento que capta a frequência correta da emissão, amplifica o sinal e recupera a

informação passando por barreiras físicas de acesso, *firewalls*, criptografia, entre outras (KOOPS, 1999). Sobre essa vulnerabilidade, será explorado no próximo capítulo o *Tempest*, um termo que nasceu durante a I Guerra Mundial e tornou-se um padrão de certificação para equipamentos militares e do governo americano nos dias atuais.

3.1.3 O *Tempest*

A primeira informação que se tem sobre o *Tempest*[10] data de 1918 (GARLICK, 2005) quando o criptologista americano Herbert Osborne Yardley, autor do livro "*The Black American Chamber*" de 1931, trabalhava como telegrafista para o Exército dos Estados Unidos. Revelou que os códigos usados pelo Governo eram fracos, pois já haviam sido criados havia dez anos e eram facilmente decodificados. Ele relatou esses fatos e convenceu o Governo a criar um serviço especializado em quebrar códigos de outros países durante a I Guerra Mundial. Vários métodos foram desenvolvidos para interceptar chamadas telefônicas e transmissões de rádio secretas. Nesse ponto, foi descoberto que os equipamentos da época tinham uma variedade de deficiências técnicas no qual possibilitavam informações serem captadas pelo inimigo através de emissões eletromagnéticas.

Tempos depois, relata Garlik (2005), em 1942, durante a II Guerra Mundial, o governo americano desenvolvia um teletipo chamado Sigaba, uma espécie de máquina de escrever elétrica dotada de recursos para criar mensagens codificadas o eficiente para superar a criptoanálise dos inimigos alemães e japoneses. Mas, um engenheiro que participava do projeto, notou que um equipamento próximo, um osciloscópio, captava cada tecla digitada gerando picos que poderiam posteriormente revelar todo o segredo da criptografia das mensagens enviadas. Ele chamou esse fenômeno de *Tempest*. Em decorrência desse fato, a companhia americana Bell Telephone, antecessora da AT&T, e que fornecia equipamentos de comunicação ao Governo dos EUA, foi questionada sobre a segurança destes aparelhos. Posteriormente, colocada à prova pela Signal Corps, uma agência de inteligência do Exército, foi procedido testes com engenheiros da Bell e conseguiu se reproduzir, a uma distância de oitenta metros, mais da metade do texto processado quatro horas depois de transmitido (SINGEL, 2008).

[10] Algumas literaturas sugerem que *Tempest* é um acrônimo ou mesmo a tradução literal de 'tempestade', vinculado ao fato que a mesma causa interferências eletromagnéticas. Mas, oficialmente, o Governo dos Estados Unidos nega essas especulações afirmando que *Tempest* é apenas um nome (GARLICK, 2005).

Em 1972, um documento secreto da NSA (ESTADOS UNIDOS DA AMÉRICA, 1972), intitulado de *"Tempest: a signal problem"*, vai descrever tudo o que foi comprovado sobre vulnerabilidades de segurança através de emissões comprometedoras geradas pelos equipamentos. Isso forçou o Governo dos Estados Unidos a emitir normas rigorosas para blindagem de todos os aparelhos, desde computadores, rádios, monitores até a criptografia de sinal dos telefones móveis. Tudo o que foi relacionado a estas normas, medidas, contramedidas e série de estudos foram chamados pelas agências de segurança e Governo americano de *Tempest*, o qual passou a ser um padrão de certificação para equipamentos homologados para o Governo (ESTADOS UNIDOS DA AMÉRICA, 2009).

Até aquele momento, apenas os órgãos de Governo como os Estados Unidos, Japão e União Soviética tinham conhecimento sobre citada falha de segurança. A primeira informação pública conhecida (VAN ECK, 1985) foi por meio do pesquisador holandês Wim van Eck que publicou um artigo em 1985, chamado *"Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?"* (Emissões Eletromagnéticas geradas por Equipamentos de Vídeo: um risco de escutas?) explicando como era possível captar e reexibir linha a linha a imagem de monitores modificando equipamentos comuns como videocassetes, televisores, antenas e aparelhos de medição de sinais. O artigo repercutiu pelo mundo e desencadeou várias pesquisas sobre o assunto. Sua pesquisa ficou conhecida como 'ataque *Tempest*' ou mesmo '*Van Eck Phreaking*'.

3.1.4 Vulnerabilidades

Em 1998, no laboratório de computação da Universidade de Cambridge no Reino Unido, os pesquisadores Markus G. Kuhn e Ross J. Anderson (KUHN, 1998) exibiram um estudo sobre a possibilidade de transmissão de dados por vias eletromagnéticas de forma camuflada e involuntária como se faz na esteganografia[11]. Kuhn, posteriormente, contribuiu com diversas pesquisas na área. Publicou um relatório técnico (KUHN, 2003) no qual documentou e atualizou o assunto. Patenteou um *software* capaz de detectar programas não licenciados, instalados em computadores, através de transmissão eletromagnética

[11] Esteganografia, do grego 'escrita oculta': método empregado desde a antiguidade para o envio de mensagens camufladas. Hoje, sua versão digital permite esconder qualquer arquivo (figura, texto, som) dentro de outro arquivo, aproveitando lacunas não significativas de bits, de forma que fique imperceptível para quem defronta o arquivo. É bastante usado para ocultar marcas d'água digitais (DEITEL, 2002).

(KUHN, 2011). Descobriu ainda que era possível aplicar o *Tempest* em conexões de vídeo digitais DVI-D e HDMI e nos recentes monitores de LCD.

Essa descoberta foi divulgada em um simpósio apresentado em 2011 (KUHN, 2011), nos Estados Unidos, com o tema*: "Compromising Emanations of LCD TV Sets"*. Até então, era controverso o fato de ser possível receptar apenas as transmissões analógicas, principalmente de cabos de má qualidade e monitores de tubo (CRT – *Cathode ray tube* ou tubo de raios catódicos) no qual as emissões eletromagnéticas são mais potentes. Com o estudo, contestou-se que, mesmo em monitores LCD e similares, há um circuito que converte o sinal digital em analógico para seja legível para o ser humano e, justamente nessa conversão, o sinal pode ser captado. Isso aconteceu, como cita, na eleição da Holanda em 2007, quando um intruso capturou a certa distância o que era exibido na tela de uma urna eletrônica.

Conexões como a DVI-D e a HDMI são totalmente digitais (WILSON, 2008) e seus cabos transmitem o sinal para os monitores utilizando o protocolo TMDS (*Transmition Minimized Differential Signalling* ou sinalização diferencial minimizada pela transição) e mesmo utilizando algoritmos complexos, podem ser decodificados se feita uma análise criteriosa dos sinais captados (KUHN, 2003).

O jornal brasileiro O Estado de São Paulo (SCAGLIA, 1998) publica matéria sobre o assunto apontando as falhas de segurança incomuns, mas perigosas, que podem ocorrer caso não sejam tomadas medidas corretivas e preventivas no ambiente computacional. Destaca que, nada vale criptografia e outras barreiras lógicas, se a emissão eletromagnética gerada por impressoras, monitores e teclados tolera ser captada e decodificada a distância. Relata que um equipamento similar ao *Tempest* poderia ser construído por qualquer pessoa com bons conhecimentos em eletrônica de rádio e televisor e, na época, havia um sistema completo disponível para ser comprado pela *internet* (ANEXO).

Na Suíça, dois pesquisadores (VUAGNOUX, 2009) conduziram experimentos sobre o eletromagnetismo emitido por teclados comuns de computador[12]. Martin Vuagnoux e Sylvain Pasini, doutorandos do LASEC - *LAboratoire de SÉcurité et de Cryptographie*, da Escola Politécnica Federal de Lausanne, notaram que os métodos anteriores para captar as

[12] Pesquisa realizada com teclados fabricados de diversas marcas e modelos entre 2001 e 2008. A documentação foi publicada no 18th USENIX Security Symposium 2009 em Montreal no Canadá e recebeu premiação do Outstanding Student Paper Award (USENIX 2009).

radiações emitidas não procediam a resultados satisfatórios. Isso porque, a dinâmica da captura envolve diversos fatores como obstáculos naturais, implicação de outras radiações no ambiente e uma gama de frequências possíveis que um teclado pode dissipar dificultando a sintonização da frequência exata dos sinais.

3.1.5 Experimentos

A partir de pesquisas realizadas no LASEC (VUAGNOUX, 2008), Vuagnoux e Pasini desenvolveram um *software* capaz de converter a frequência de cada tecla digitada em seu caractere correspondente formando o texto ou combinação de teclas com precisão muito alta. Os equipamentos empregados para captação dos sinais eram relativamente simples e baratos, dentre eles, uma antena de rádio e um receptor de frequências ampliadas Os experimentos foram feitos em várias distâncias e com diversas marcas de teclados, com e sem fio, tomando o cuidado de isolar outras fontes de radiação eletromagnética. Para isso, utilizaram um *laptop* com o monitor desligado (no momento do teste) e alimentado apenas com a bateria, sem o carregador, e assim introduzindo os teclados a serem testados nas entradas correspondentes (conexões PS/2 ou USB). Foi possível, nessas condições, obter sucesso na captação das teclas digitadas em uma sala distante vinte metros do teclado experimental, mesmo através das paredes do ambiente. Cada um dos teclados sofreu quatro ataques pré-determinados pelos pesquisadores, incluindo o método de Kuhn e Anderson, e todos foram vulneráveis ao menos um dos métodos utilizados.

> "Concluímos que os teclados com fios vendidos nas lojas geram emanações comprometedoras (principalmente por causa das pressões dos custos de fabricação), por isso, eles não são seguros para transmitir informações sensíveis e confidenciais. Sem dúvida nossos ataques podem ser significativamente melhorados, uma vez que usamos um equipamento relativamente barato", Martin Vuagnoux e Sylvain Pasini (VUAGNOUX, 2008).

No Brasil, o Tribunal Superior Eleitoral realizou, em 2009, a primeira edição do evento “Testes Públicos de Segurança do Sistema Eletrônico de Votação” (BRASIL, 2009a), cujo objetivo foi oferecer a oportunidade para que qualquer pessoa testasse possíveis vulnerabilidades da urna eletrônica. Sérgio Freitas da Silva, um dos consultores inscritos, utilizou os princípios de Van Eck e Vaugnoux captando as emissões eletromagnéticas geradas pela urna eletrônica e demonstrou ser possível quebrar o sigilo eleitoral do equipamento:

> "Fiz meu experimento em 29 minutos e obtive sucesso no escopo que estava proposto: rastrear a interferência e gravar arquivos para comprovar a materialidade do fenômeno, que sintonizam ondas longas e curtas e estações em AM e FM. Enquanto eu digitava na urna, rastreava através do rádio pra ver se detectava alguma interferência. Consegui rastrear a interferência que isto provocava na onda, gravando um arquivo WAV[13]com estes sons e após gravar os ruídos que os botões da urna eletrônica exercem sobre a onda é possível decodificar os sons, o que levaria à descoberta dos candidatos escolhidos pelo eleitor, quebrando seu sigilo. É como se o teclado da urna eletrônica se transformasse em um teclado musical, conseguindo rastrear a tonalidade da interferência neste arquivo WAV que gravei", Sérgio Freitas da Silva (FELITTI, 2009).

Silva procedeu ao teste utilizando um aparelho de rádio comum (BRASIL, 2009b) enquanto digitava repetidas vezes uma tecla qualquer da urna eletrônica. Ele conseguiu sintonizar uma frequência em que era possível ouvir um ruído provindo da emissão eletromagnética gerada pela tecla digitada. Isso já garantiu sua premiação, pois seria possível gravar esses sons no computador, analisar as variações das ondas e assim criar um padrão para as treze teclas da urna revelando todo o processo de votação. Apesar de posicionar o rádio a uma distância de alguns centímetros da urna, comentou que seria possível distâncias bem maiores utilizando equipamentos e antenas mais potentes como realizado na Suíça pelos pesquisadores Martin Vaugnoux e Sylvain Pasini, citados anteriormente. Essa vulnerabilidade da quebra de sigilo do voto é confirmada pelo especialista em segurança Marco Canut, que presta consultoria ao Governo:

> "Todo computador é uma pequena estação de rádio, emitindo ondas eletromagnéticas. Enquanto os humanos notam como um chiado, a interferência pode ser 'entendida' por máquinas, demonstrando qual a tecla escolhida pelo eleitor. Durante a Guerra Fria, o exército dos Estados Unidos descreveu os perigos da interceptação de ondas eletromagnéticas em documentos conhecidos como *Tempest*, nome que acabou se tornando o apelido da técnica. Desde então, as instalações militares norte-americanas usam técnicas que as blindam do vazamento eletromagnético", explica Canut (BRASIL, 2009b).

Canut sugere que os teclados das urnas deveriam ser substituídos por telas sensíveis ao toque, menos propensas a emitir ondas eletromagnéticas (BRASIL, 2009b), já que a blindagem, nesse caso, dificultaria a manutenção e deixaria as urnas mais pesadas, além de mais caras. Após a conclusão do evento, o Tribunal Superior Eleitoral divulgou que nenhum ataque foi bem sucedido, contrariando os testes alcançados por Sérgio Freitas da Silva. Em

[13] Arquivos Wave são gravações de áudio feitas em computador provindas de sistemas da Microsoft e não sofrem compactação, como arquivos MP3, formando uma onda de frequência pura representada em *softwares* específicos, no qual é possível detectar as variações de cada tecla digitada como apresentado nos testes.

defesa, o secretário de tecnologia do Tribunal, Giuseppe Gianino, comentou que seria impraticável um ataque similar ao realizado no evento, já que seria necessário estar próximo à urna, o que é proibido, além de estar sobre o cuidado dos mesários. E a possibilidade de utilizar equipamentos mais potentes a distância, como levantou Sérgio, defendeu que seria relativo ao campo teórico, pois senão os inscritos teriam assim apresentado algo na oportunidade que tiveram.

A hipótese foi confirmada pelo consultor Sérgio Freitas da Silva (BRAUN, 2009) sobre não utilizar os equipamentos sugeridos acrescentando que, na prática, quanto mais distante da urna, maior o risco de captar interferências de aparelhos como computadores, celulares, veículos, antenas, torres de energia. Além de as paredes, muros e prédios dispersarem e atenuarem o sinal. No auditório no qual foi realizado o evento, foram afastados equipamentos e computadores e desligada a rede sem fio, minimizando possíveis interferências.

> "Sem surpresa em ambos os testes, os criadores da urna negam a possibilidade de identificação do voto do eleitor através da captura de ondas eletromagnéticas nos teclados. Mas, sem nenhuma comprovação, somente versões pessoais dos fatos minuciosamente construídas para recolocar o resultado no caminho por eles idealizado", comenta a advogada Maria Aparecida Cortiz, especialista em auditoria de processo eleitoral (CORTIZ, 2010).

No ano seguinte, o Tribunal Superior Eleitoral adquiriu novas urnas eletrônicas com várias melhorias internas, incluindo biometria em alguns lotes (SOARES, 2010). Em 2012, aconteceu a segunda edição do evento "Testes Públicos de Segurança do Sistema Eletrônico de Votação" (BRASIL, 2012a), como ilustra a figura 11.

Figura 11 - Capa do manual do evento federal sobre segurança do sistema eletrônico de votação.
Fonte: Tribunal Superior Eleitoral (BRASIL, 2012a).

Os participantes tiveram acesso à *internet* e ao código-fonte da urna na íntegra, além da oportunidade de ter contato com o *software*, o *hardware* - incluindo a placa-mãe, os componentes eletrônicos e outros dispositivos internos (BRASIL, 2012b). Apesar da

conveniência para que os inscritos pudessem ousar mais em seus experimentos, desta vez não foi encontrada nenhuma vulnerabilidade no sistema (BRASIL, 2012c).

3.1.6 Certificações de blindagem

Atualmente, o termo EMSEC (*Emissors Security*) passou a ser mais usual em documentos governamentais americanos (ESTADOS UNIDOS DA AMÉRICA, 2009), em substituição ao *Tempest*, englobando todas as medidas de segurança conhecidas e adotadas em equipamentos e sistemas de informação automatizados (AIS) evitando que informações sigilosas sejam interceptadas por pessoas não autorizadas (GARLICK, 2005). O termo *Tempest* agora designa o padrão de equipamentos eletroeletrônicos fabricados nos Estados Unidos certificados de acordo com o nível de emissão de eletromagnetismo dissipado em três categorias (BLACK BOX, 2012): *Tipo 1* - extremamente seguro com criptografia classificada para fins de segurança nacional, disponível somente para o alto governo dos Estados Unidos; *Tipo 2* - também com criptografia, mas não classificada, acessível apenas para os governos estaduais e locais, agências de inteligência e segurança e algumas empresas qualificadas; *Tipo 3* - para equipamentos com criptografia não classificada de uso comercial, onde é executado um algoritmo registrado no Instituto Nacional de Padrões e Tecnologia (NIST), sendo usado na proteção de informação confidencial, como comunicações de uma corporação de rede. A figura 12 mostra um equipamento utilizado no exército britânico. No detalhe acima à direita, a advertência para não operar o equipamento com sua porta aberta sob o risco de comprometer a integridade da emissão *Tempest* com poeira ou umidade. Abaixo, em outro detalhe, um selo de certificação *Tempest*.

Figura 12 - Fotografia de um equipamento militar utilizado no Reino Unido com certificação Tempest. Fonte: IARRCIS EXI, 2011.

4 ENSAIO SOBRE A VULNERABILIDADE DA INFORMAÇÃO

Neste capítulo, serão apresentados ensaios com base na descrição do levantamento teórico pesquisado. Tendo como escopo investigar a vulnerabilidade do vazamento de emissão eletromagnética de componentes de informática, serão montados três ambientes dispostos de equipamentos comuns, como aparelhos de rádio e computadores com o *software* responsável por gerar o sinal enviado ao monitor. Esse sinal deverá causar emissão eletromagnética de forma harmônica, ou seja, em formato de música, no qual poderá ser captada pelo aparelho de rádio.

O *software* tem plataforma Linux e é baseado no programa *Tempest AM*, escrito pelo programador finlandês Pekka Riikonen (RIIKONEN, 2001), o qual foi modificado pelo pesquisador alemão Erik Thiele (TEMPEST FOR ELIZA, 2001). Thiele compilou a música clássica *Für Elise* de Beethoven (domínio público) para ser gerada como sinal e acrescentou um *script* que possibilita rodar outras músicas de formato *wave* ou MP3.

Não há exigências de configuração recomendada para o computador, já que o sistema operacional e o *software* rodam com menos de 500 MB de memória RAM em ambiente gráfico. Assim, serão empregados um computador tipo *desktop* e outro móvel (*laptop*) cada um com dispositivo reprodutor de CD ajustado para preceder a inicialização. O disco rígido será necessário apenas para armazenar o *software Tempest for Eliza* (44 kB), já que a plataforma Linux utilizada será por Live-CD, portanto, sem instalação. Os aparelhos de rádios são simples e capazes de sintonizar a faixa de ondas médias, conhecida por AM.

4.1 O ambiente

Para simulação dos testes propostos, serão aplicadas diferentes configurações buscando obter uma gama de resultados para posterior comparação. A seguir, a lista dos equipamentos empregados e suas configurações:

AMBIENTE 1:

- computador com processador AMD Athlon 2200 XP, 2 GB de memória RAM, 120 GB de disco rígido, placa de vídeo *offboard* VGA Sis, drive de CD;
- monitor LG LCD 21” com cabo VGA comum sem blindagem;

- rádio *system* AIWA com sintonização para ondas médias (AM);
- sistema operacional Linux Slax versão 6.1.2 Live-CD;
- *software Tempest for Eliza* disponibilizado no disco rígido.

AMBIENTE 2:

- *laptop* Acer Aspire 3000, processador AMD Sempron 3100+, 1 GB de memória RAM, 80 GB de disco rígido, placa de vídeo VGA Sis, drive de CD, monitor LCD 15".
- rádio-relógio Powerpack com sintonização para ondas médias (AM);
- sistema operacional Linux Slax versão 6.1.2 Live-CD;
- *software Tempest for Eliza* disponibilizado no disco rígido.

AMBIENTE 3:

- Idem ao ambiente 2, apenas alterando para o rádio automotivo Honda/Panasonic.

CONFIGURAÇÕES DOS AMBIENTES

a) Ajuste de três sintonizações distintas do *software* dentro da faixa de ondas médias compreendidas entre 520 a 1610 kHz;
b) Proximidade do aparelho de rádio para 1 cm, 100 cm e 300 cm do computador;
c) Troca do cabo VGA comum para um cabo VGA blindado (somente ambiente 1).

4.2 Testes

Disposto de todo material necessário, será realizada uma rotina de procedimento comum a todos os testes:

1) Carregamento do sistema operacional Linux, distribuição Slax, em plataforma gráfica KDE, via Live-CD. O Slax, por padrão, já inicia como usuário root ($);
2) Obter, gravar e disponibilizar para execução o *software Tempest for Eliza* (TEMPEST FOR ELIZA, 2001) no disco rígido. Por padrão, estará no diretório: /usr/bin
3) Descompactar o arquivo do *software* no local gravado usando o *Terminal* com o seguinte comando:

   $ tar -zxvf tempest_for_eliza-1.0.5.tar.tar

4) Compilar o *software* entrando no diretório criado e executando o respectivo *script*:

   $ cd /usr/bin/tempest_for_eliza-1.0.5/

   $ ./configure

5) Carregar o *software*:

   $ make

6) Agora, será preciso colher alguns dados exigidos do monitor de vídeo empregado. Para isso, é carregado o programa nativo Linux (nesta distribuição), o Xvidtune:

   $ xvidtune

7) Com a janela apresentada, no exemplo da figura 13, será necessário verificar os seguintes valores fornecidos: *Hdisplay, Vdisplay, Htotal e Pixel clock*. Anotar os valores e fechar essa janela;

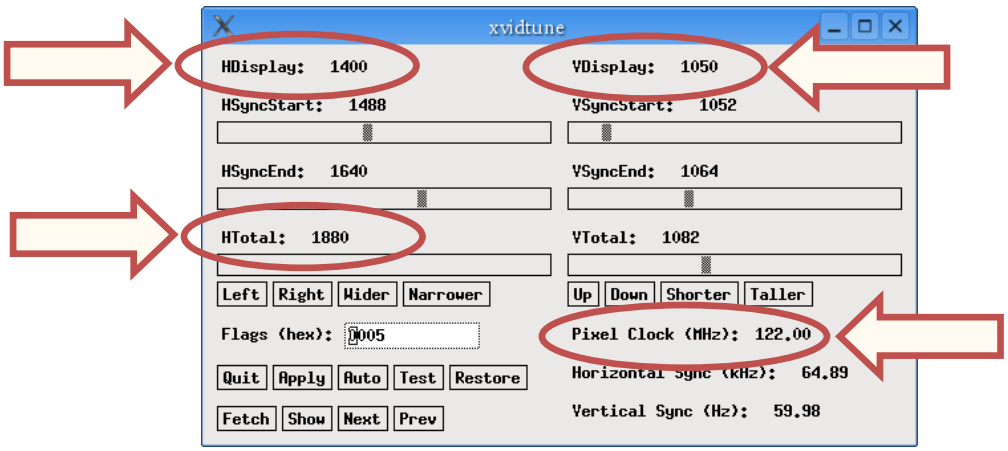


Figura 13 - Imagem da janela de configuração do programa Xvidtune.
Fonte: Reprodução de Slax, 2009.

8) Por último, escolher um valor entre 520 a 1610 kHz, que representa a faixa de ondas médias do rádio. O ajuste da sintonização deverá ser em uma faixa em que não haja estações próximas, ou seja, o som será apenas do chiado característico. Isso varia de acordo com o espaço onde está situado o aparelho de rádio. Como parâmetro, os valores escolhidos estarão sintonizados no início, meio e final da faixa disponível;

9) Desta maneira, o comando será executado da seguinte forma:

   $ ./tempest_for_eliza (Pixel clock) (Hdisplay) (Vdisplay) (Htotal) (faixa AM) songs/forelise

10) Para esclarecer esse comando, utilizar como exemplo os valores da figura 13:

- Hdisplay = 1400

- Vdisplay = 1050

- Htotal = 1880

- Pixel clock[14] = 122 000 000

- Estação escolhida[14] = 520 000

Aplicando os valores ao comando exato ficaria:

$ ./tempest_for_eliza 122000000 1400 1050 1880 520000 songs/forelise

4.2.1 Teste do ambiente 1

O procedimento inicial desse teste será ligar os equipamentos listados no capítulo 3.1, nesse caso, o computador desktop e aparelho de rádio como esquematizado na figura 14 e apresentado na figura 15. O ajuste da inicialização do computador já está configurado para carregar primeiramente o *drive* de CD e assim o sistema operacional Linux Slax. Durante o carregamento do sistema são listadas as plataformas disponíveis, então se escolhe a plataforma gráfica (*Slax Graphic Mode - KDE*). Poderá ser escolhida a opção de modo texto (*Slax Text Mode*), principalmente se fosse utilizado computador com pouco processamento e memória. Nada impede que seja aproveitada outra distribuição Linux, portanto que inclua e tenha instalado o programa Xvidtune ou compatível para obter os valores necessários do monitor e ser possível rodar o *software Tempest for Eliza*. A partir daqui, segue-se o procedimento do capítulo 3.2.

Os valores encontrados pelo Xvidtune para esse monitor são:

- Hdisplay = 1680

- Vdisplay = 1050

- Htotal = 1840

- Pixel clock = 119 000 000

- Estações escolhidas: 550 000 /1 200 000 / 1 600 000.

Deste modo, o comando executado será o seguinte:

$ ./tempest_for_eliza 119000000 1680 1050 1840 550000 songs/forelise

[14] Em virtude de o valor ser representado em MHz (um milhão de Hertz), considerar o valor integral seguido de seis zeros. O mesmo caso para a estação escolhida em kHz (mil Hertz), o número integral deve seguido de três zeros.

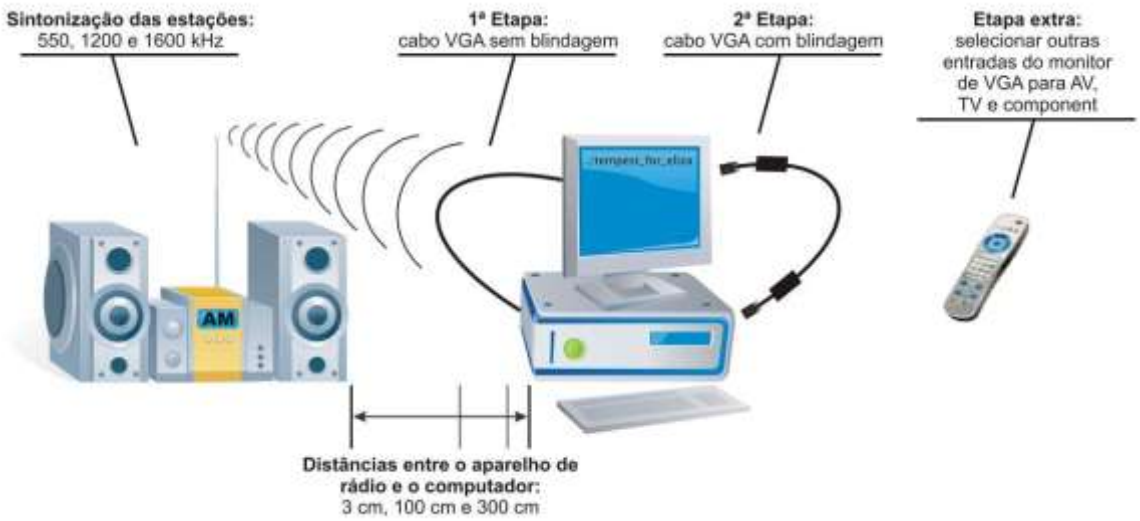


Figura 14 - Ilustração do plano montado para o ambiente 1.
Fonte dos ícones: artshare.ru, 2008 (licença CC 3.0). Montagem própria.

Todos os testes deste ambiente se darão desta forma, bastando apenas substituir o último valor pela estação escolhida. Ao executar o comando, o aparelho de rádio deverá ser sintonizado próximo ao valor determinado para que se possa ouvir a música correspondente. Serão testadas três distâncias do aparelho de rádio ao computador: um, cem e trezentos centímetros, aguardando o final de cada execução do programa para alterar as distâncias. A primeira etapa será com um cabo de monitor VGA comum e na etapa posterior um cabo semelhante, mas com blindagem. Uma etapa extra irá alterar as entradas disponíveis do monitor (TV, AV e componente) durante o teste.

Figura 15 - Fotografia sobre a disposição do ambiente 1.
Fonte própria.

A tabela 3 apresenta os valores coletados nos testes do ambiente 1:

Tabela 3 - Resultado dos testes do ambiente 1.

CABO	SINTONIZAÇÃO EM kHz	DISTÂNCIA EM cm	SUCESSO
Comum	550	1	Sim
		100	Não
		300	Não
	1200	1	Sim
		100	Não
		300	Não
	1600	1	Sim
		100	Não
		300	Não
Blindado	550	1	Sim
		100	Não
		300	Não
	1200	1	Sim
		100	Não
		300	Não
	1600	1	Sim
		100	Não
		300	Não

Fonte própria.

4.2.2 Teste do ambiente 2

Após ligar os equipamentos correspondentes aos listados no capítulo 3.1, agora com um *laptop* utilizando seu próprio monitor, como esquematizado na figura 16 e apresentado na figura 17, será executada a rotina de procedimentos do capítulo 3.2. O computador já está configurado para carregar primeiramente o *drive* de CD e assim o sistema operacional Linux Slax. Os valores encontrados pelo Xvidtune para esse monitor são:

- Hdisplay = 1280
- Vdisplay = 800
- Htotal = 1688
- Pixel clock = 107 860 000
- Estações escolhidas: 640 000 /1 300 000 / 1 470 000.

Deste modo, o comando executado será o seguinte:

$ ./tempest_for_eliza 107860000 1280 800 1688 640000 songs/forelise

Figura 16 - Ilustração do plano montado para o ambiente 2.
Fonte dos ícones: Artshare.ru, 2008 (licença CC 3.0). Montagem própria.

Todos os testes deste ambiente se darão desta forma, bastando apenas substituir o último valor pela estação escolhida. Ao executar o comando, o aparelho de rádio deverá ser sintonizado próximo ao valor determinado para que se possa ouvir a música correspondente. Serão testadas três distâncias do aparelho de rádio ao computador: um, cem e trezentos centímetros, aguardando o final de cada execução do programa para alterar as distâncias.

Figura 17 - Fotografia sobre a disposição do ambiente 2.
Fonte: própria.

A tabela 4 apresenta os valores coletados nos testes do ambiente 2:

Tabela 4 - Resultado dos testes do ambiente 2.

SINTONIZAÇÃO EM kHz	DISTÂNCIA EM cm	SUCESSO
640	1	Sim
	100	Não
	300	Não
1300	1	Sim
	100	Não
	300	Não
1470	1	Sim
	100	Não
	300	Não

Fonte própria.

4.2.3 Teste do ambiente 3

No ambiente esquematizado na figura 18 e apresentado na figura 19, foi empregado o mesmo *laptop*, portanto serão usados os mesmos valores do Xvidtune, alterando as estações para: 700 000 / 910 000 / 1550 000. Neste caso, o aparelho de rádio será automotivo utilizando o próprio veículo como plataforma, segundo correspondente ao ambiente 3 no capítulo 3.1. O *laptop* será posicionado externamente no teto do veículo próximo à antena do aparelho de rádio (figuras 18 e 19).

Figura 18 - Ilustração do plano montado para o ambiente 3.
Fonte dos ícones: Supreetstation, 2010 (licença CC 3.0). Montagem própria.

Figura 19 - Fotografias sobre a disposição do ambiente 3: à esquerda a acomodação do *laptop* em cima do veículo próximo à antena externa e, à direita, o aparelho de rádio instalado na parte interna do veículo.
Fonte própria.

A tabela 5 apresenta os valores coletados nos testes do ambiente 3:

Tabela 5 - Resultado dos testes do ambiente 3.

SINTONIZAÇÃO EM kHz	DISTÂNCIA EM cm	SUCESSO
700	1	Sim
	100	Não
	300	Não
910	1	Sim
	100	Não
	300	Não
1550	1	Sim
	100	Não
	300	Não

Fonte: própria.

Para explanação do que foi descrito nos testes, como a execução dos *script*s, o ruído gerado pela emissão eletromagnética nos rádios e o efeito de sincronização na tela dos monitores, uma síntese da apresentação foi gravada em vídeo e está disponível para ser visualizada em PATRÍCIO (2012).

5 DISCUSSÃO DOS RESULTADOS

De maneira geral, os testes realizados alcançaram o objetivo de demonstrar a emissão eletromagnética irradiada, na qual continham dados que seriam passíveis de interceptação conduzidos pelo próprio ar. Este capítulo irá debater o desenvolvimento dos testes em relação ao levantamento teórico apresentado.

5.1 Captação de sinais por meio de cabos externos

A baixa potência dos aparelhos de rádio utilizados nos testes foi um fator chave para ilustrar que a fuga dos sinais nos cabos é mínima necessitando estar praticamente encostado ao computador para obter a captação, como mostram as tabelas do capítulo 3. Mas, isso seria revertido com aparelhos mais potentes que suportassem antena externa amplificada, aumentando consideravelmente a distância entre os equipamentos para a captação do sinal.

Esse foi o caso dos experimentos realizados por Vuagnoux e Pasini na Suíça, descritos no capítulo 2.4.6. Nos vídeos gravados, disponíveis em Vuagnoux (2008), observam-se aparelhos mais elaborados para análise de sinais e uma antena bicônica (figura 20), específica para captação de interferências eletromagnéticas. Para tanto, conseguiram captar sinais distantes a vinte metros dos teclados de computador em ambiente fechado, atravessando paredes e outras barreiras, ainda assim, explicaram que a captação poderia ser aprimorada com equipamentos mais sofisticados. Isso contradiz os comentários de Gianino e Silva sobre a vulnerabilidade das urnas eletrônicas no capítulo 2.4.6 (BRAUN, 2009), justificando que ataques desse tipo são impraticáveis pelo fato do alcance de sinal e de interferências captadas, sendo possível seu funcionamento apenas em teoria.

Figura 20 - Fotografia de uma antena tipo bicônica.
Fonte: KUHN, 2003.

A tecnologia utilizada nos teclados de computador é muito mais simples se comparada aos monitores. Teclados comerciais remetem ao início da era PC, no final da década de 1970 e mudaram pouco internamente, assim como os monitores de cinescópio (tubo de raios catódicos ou CRT) que surgiram nos anos 1960. O cabo de teclados, independente de sua conexão (DIN, PS2 ou USB), é composto por quatro fios internos sendo dois para fornecimento de energia e dois para envio de sinais. Já o cabo VGA de monitor tem quinze fios, dois para fornecimento de energia e até treze para transmissão e retorno de sinais. A título de comparação, o teclado apenas envia dados combinados de pouco mais de cem teclas e não mais que cinco delas simultaneamente. Enquanto que, a placa de vídeo VGA precisa transmitir, do cabo ao monitor, milhares de informações simultâneas e em constante atualização para que seja possível compor a imagem na tela. Tomando por base a taxa de atualização de 60 Hz de um monitor padrão, logo a placa de vídeo irá alterar as imagens a cada 0,016 segundos (16 milissegundos, como a fórmula do capítulo 2.4.1).

Defronte às pesquisas de Vuagnoux e Pasini em relação ao programa *Tempest AM* de Riikonen (capítulo 3, utilizando o cabo de monitores como antena), constata-se que o cabo dos teclados, mesmo com o envio único de dados, emite ondas eletromagnéticas o suficiente para comprometer sua confidencialidade. Esses dados são facilmente mapeados, pois se conhece a maioria das teclas e caberia ao *software* interpretar as nuances de ondas para revelar as combinações de teclas digitadas. Além disso, um *script* incorporado ao *software* que utilize o método de consulta a dicionário para deduzir as palavras, visto que, há uma margem de erro na interpretação das ondas. Assim, a mesma base de conhecimento pode ser aplicada para captar informação provinda de cabos de monitores, porém, precisa ser mais elaborada em virtude da complexidade de dados que trafegam por esses cabos.

De tal modo, Kuhn concentrou seus estudos na captação de ondas eletromagnéticas oriundas de monitores em vários aspectos (KUHN 1998 e 2003). No caso da emissão originada por cabos, considerou duas classes: analógica e digital. O padrão VGA, mostrado na figura 21 com detalhe do conector na figura 22 à esquerda, e anteriores são analógicos, partindo da placa de vídeo, que recebe os dados digitais brutos da memória e do processador e os converte em sinais analógicos para então serem enviados ao monitor. Por esse fato, o sinal fica mais suscetível às emissões e mais simples de ser identificado, já que vem de uma tecnologia defasada.

No teste do ambiente 1 no capítulo 3, a conexão VGA foi aplicada utilizando um cabo comum e outro blindado com anéis de ferrite próximos aos conectores (figura 21). Essa blindagem tem o propósito de minimizar a emissão eletromagnética, como aconselhado em um simpósio ministrado por Kuhn, (2011). Mas, na prática, não houve efeito de atenuação e o resultado do teste com os dois tipos de cabos foi praticamente idêntico (tabela 3). Uma causa provável para esse fato deve-se aos materiais de fabricação dos cabos não serem de boa qualidade. O diâmetro mais fino denuncia que os fios internos têm condução fraca da corrente elétrica e provavelmente não possuem uma malha de metal que envolve todo o cabo e interliga os conectores, como presente nos cabos coaxiais. Essa malha é importante para a blindagem elétrica (aterramento) dos equipamentos interligados, um método eficaz para atenuar ruídos de sinal e, por consequência, minimizar a emissão eletromagnética.

Figura 21 - Fotografia de cabos VGA com gomos nos quais estão embutidos os anéis de ferrite.
Fonte: Catálogo Black Box, 2012.

Padrões posteriores como o DVI-D[15] e HDMI são inteiramente digitais (detalhe dos conectores na figura 22), portanto não necessitam de conversão analógica/digital e ainda incluem o protocolo TMDS que codifica sua transmissão (WILSON, 2008). Apesar desse cuidado, Kuhn detectou o algoritmo desse protocolo e conseguiu decodificá-lo (KUHN 2003).

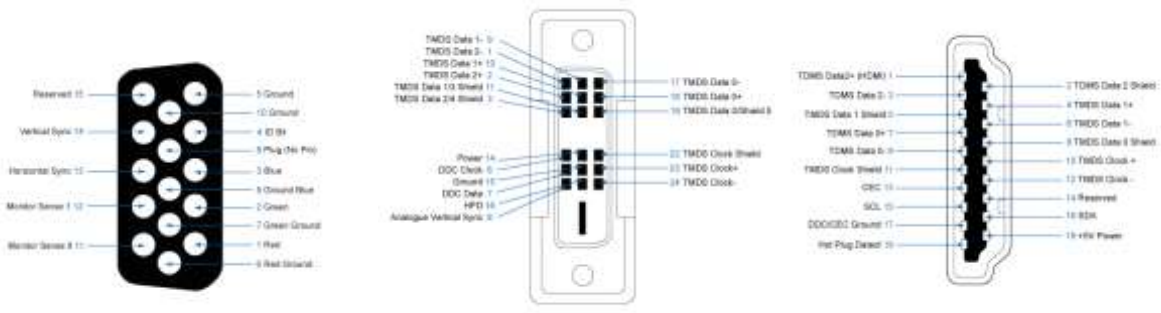


Figura 22 - Desenhos de conectores de vídeo, da esquerda para direita: VGA, DVI-D e HDMI.
Fonte: Catálogo Black Box, 2012.

[15] A primeira geração do padrão DVI era híbrida: analógica e digital. O HDMI é junção do DVI-D com conexões de áudio. Diversos outros padrões de vídeo digitais foram criados, mas são menos conhecidos.

Porém, o protocolo mais recente HDCP[16] (figura 23), foi criado com o intuito de evitar a cópia de vídeos em alta definição e proteger os direitos autorais das produtoras de mídia. Entretanto, mostrou ser eficiente na confidencialidade dos dados transmitidos pelos cabos por empregar criptografia e desse modo, segundo Kuhn, sua receptação é plausível, mas os dados captados não seriam legíveis.

O HDCP é um protocolo de autenticação: equipamentos de vídeo recentes[17] que possuem conexão digital (DVI-D / HDMI) e são certificados pelo HDCP, vêm de fábrica com chaves de identificação e algoritmos de codificação e decodificação armazenados em suas memórias para efetuarem um processo de criptografia chamado *handshake* (WILSON, 2008). A conexão será efetivada entre um equipamento fonte, que gera o sinal, e um equipamento receptor. Tomando como exemplo um aparelho de *blu-ray* (fonte) conectado via HDMI em um televisor (receptor), o *blu-ray* inicialmente codifica seus dados e gera uma chave comparando a seguir com a chave de autenticação do televisor. Caso as chaves estejam corretas, o televisor irá utilizar essas chaves, codificá-las e retornar uma nova chave de autenticação da qual será compartilhada com o *blu-ray* para criptografar a transmissão.

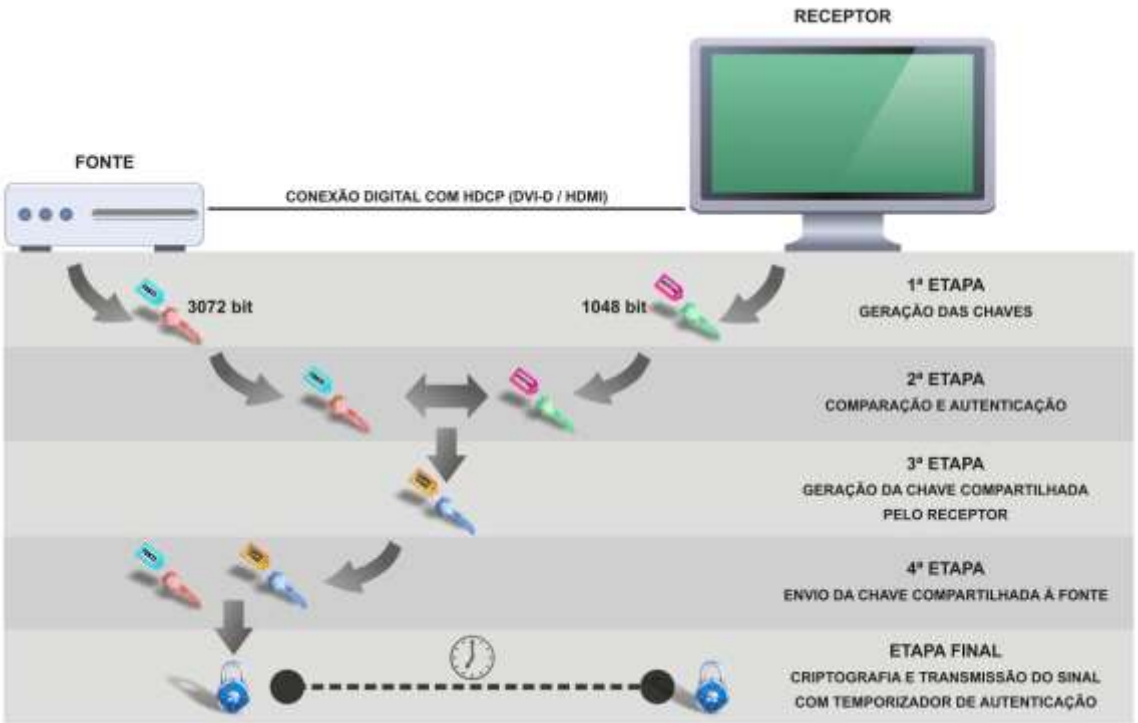


Figura 23 - Ilustração sobre o processo de *handshake* (criptografia) de uma conexão HDCP versão 2.2. Fontes dos ícones: Artshare.ru, 2008 e Simiographics, 2012 (licença CC 3.0). Montagem própria.

[16] HDCP: proteção de conteúdo digital em banda larga - desenvolvido pela Intel desde 1990 e homologado em 2003. Sua adesão pelos fabricantes é facultativa, porém não será compatível com equipamentos certificados.
[17] Equipamentos de vídeo de alta definição: televisores, videojogos, monitores, tocadores de disco *blu-rays*, decodificadores de sinal a cabo e satélite, projetores, *laptop*s e placas de vídeo.

Por fim, estabelecida a autenticação dos equipamentos, haverá um ciclo periódico de revisões para certificar se a conexão está segura e nenhuma das chaves ou equipamentos foram alterados. Qualquer mudança não prevista fará interromper a transmissão. A tentativa de conectar a fonte em um aparelho que faça gravações de vídeo ou que não seja certificado HDCP restringirá a autenticação ou exibirá o vídeo em resolução inferior.

Apesar do empenho em se criar um protocolo seguro no qual o material com direitos autorais esteja protegido, o HDCP também foi violado e sua chave mestra, o segredo de todo o processo de sua criptografia, descoberta em 2010, com reconhecimento da Intel.

Portanto, os cabos externos de periféricos de informática necessitam de procedimentos eficazes na transmissão de sinais e componentes mais elaborados em sua fabricação que atenuem ao máximo a emissão eletromagnética.

5.2 Captação de sinais por meio de cabos internos

Os testes finais nos ambientes 2 e 3 (capítulo 3), empregando o mesmo *laptop*, apresentaram pontos diferentes de fuga de sinal. Inicialmente, no ambiente 2, o aparelho de rádio não conseguiu nenhum vestígio de sinal, mesmo mudando de cômodo, trocando as posições em volta ao *laptop* e alterando as frequências do *script* e da sintonização. Enfim, a posição capaz de ajustar o sinal foi próximo à fonte de energia do *laptop*, no lado direito junto à dobradiça do monitor, como mostrado na figura 17, no qual o rádio-relógio está exatamente encima desse local. Para isolar o fato de ser o carregador de energia o responsável pela emissão, este foi desconectado do *laptop* e o equipamento ficou alimentado apenas com a bateria, o que atenuou o sinal pela metade, mas permaneceu audível. Isso pode ter ocorrido pelo tempo de vida da bateria que se descarrega rapidamente e não suporta mais a carga total.

Pesquisando o interior do *laptop* (figura 24) no ponto no qual foi posicionado o rádio-relógio, foi verificada a placa de vídeo instalada nesse local, o que aponta ter blindagem mínima, bem como, o cabo *flat*[18] que faz sua interligação com o monitor. De fato, não há nenhuma proteção metálica em volta da placa de vídeo e nenhum outro artifício para evitar interferências. O cabo *flat* também não possui nenhum cuidado contra emissões em sua

[18] Esse cabo *flat* ou *flex,* os fios são enfileirados um ao lado do outro de forma plana (como uma folha de papel) e envolvidos em uma película plástica levemente curva para não esmagar os fios ao abrir e fechar o *laptop*.

construção e é presumível que seja o responsável por permitir o vazamento de sinais funcionando como uma antena transmissora da mesma maneira que os cabos externos.

Além da falta de blindagem, o próprio desenho do cabo *flat* (plano) e sua posição curvada aumentam a possibilidade da emissão de ondas. E ainda, sua localização entre a bateria e a entrada do carregador pode criar um campo propício de interferências, já que a maior demanda de energia elétrica vem do monitor, conectado próximo desse local. Kuhn (2008) comenta essa hipótese em seu relatório apontando falhas na construção de *laptops*.

Figura 24 - Ilustração de componentes internos do *laptop* mais predispostos a emitir radiação eletromagnética.
Fonte do ícone: TurboMilk.com, 2010 (licença CC 3.0). Montagem própria.

Para o teste do ambiente 3, a ideia foi criar um sistema totalmente móvel sem o uso de energia da rede elétrica (corrente alternada) e com o aparelho de rádio de um veículo, pensado para diferenciar dos demais ambientes. Visto que, no campo da Física, o interior de um veículo é um bom isolante de eletricidade em virtude dos pneus de borracha e da carroceria metálica (formando uma gaiola de Faraday), seria esperado que não houvesse resultado positivo com o *laptop* dentro do veículo. E foi esse o ocorrido: primeiro com as portas e janelas fechadas e depois com todas abertas. A solução foi encontrar externamente outros locais capazes de captar o sinal e mesmo próximo à antena de rádio, no teto do veículo e alternando as frequências do *script* e do rádio, nenhuma sintonização obteve êxito.

O teste seria dado como encerrado dessa forma, mas ao fechar o *laptop*, o sinal característico da radiação se manifestou. Nesse caso, o problema não estava somente na

posição do *laptop* em relação à antena, mas no ângulo de abertura da tampa do monitor. Depois de diversas alterações, o sinal esteve mais perceptível quando o *laptop* foi levemente fechado em um ângulo próximo de setenta graus com a antena do veículo encostada praticamente na face da tela (como se fosse fechar o *laptop* com a antena dentro), demonstrado na figura 19. A partir desse ponto, as etapas propostas foram realizadas faltando deixar o *laptop* desconectado do carregador, criando o sistema móvel suportado apenas pela corrente contínua das baterias. Idem ao ambiente 2, o resultando foi a atenuação maior de emissão eletromagnética, porém ainda audível.

O fato de o ambiente 3 estar localizado em espaço totalmente externo, próximo a muitas antenas, transformadores dos postes de energia elétrica e de outros veículos com o aparelho de rádio ligado, não interferiu de modo algum nos testes. O motivo pelo qual o *laptop* ficou posicionado em ângulo para captação do sinal pode ter sido causado novamente pelo cabo *flat*. Como explicado anteriormente, a película plástica que envolve o cabo é flexível, evitando que os fios internos fiquem dobrados e danificados, permanecendo em forma curvada. Isso provavelmente criou um campo eletromagnético concentrado em volta da antena no qual o sinal foi captado.

Para excluir a possibilidade de o monitor estar interferindo na emissão, este foi desligado logo que o *script* iniciou e não apontou nenhuma mudança. O ajuste das estações no aparelho de rádio do veículo era digital e permitia selecionar cinco quilohertz por vez, diferente do sistema analógico que não apresenta esse problema. Mas foi possível perceber a mudança de tom na música do sinal captado a cada ajuste feito (PATRICIO, 2012), o que não ocorreu nos testes anteriores. Uma suposição para o acontecido se deve à faixa de frequência de uma escala musical ser em média quinhentos hertz e o ajuste das estações estar próximo disso, no caso, cinco quilohertz.

Desse modo, é compreensível que os fabricantes queiram os *laptops* cada vez mais leves, utilizando plástico na matéria-prima de seus componentes. Por outro lado, esse material não contribui para a blindagem adequada. Chapas e malhas de alumínio isolando pontos cruciais de emissão eletromagnética, como já citada, serviriam como blindagem sem comprometer o peso do equipamento. A pintura metalizada na parte interna do gabinete também poderia minimizar os efeitos. O cabo *flat* teria alguma solução se adotasse o princípio dos cabos utilizados nos antigos discos rígidos (IDE UltraDMA) no qual parte dos fios não transportam dados e simplesmente servem para o isolamento de interferências.

Para o monitor, o cabo de energia deveria ser separado do cabo *flat* e empregado o par trançado, como no padrão das redes *Fast Ethernet*, em que os fios são enrolados em pares, um com a frequência inversa do outro minimizando o vazamento de sinais.

5.3 Captação de sinais utilizando esteganografia

A técnica na qual os testes foram realizados se beneficia de outro aspecto das pesquisas de Kuhn e seu ex-professor Anderson (KUHN, 1998): a introdução da esteganografia em dispositivos que emitem radiação eletromagnética suficiente para ser captada. O exemplo básico de estenografia, ilustrado na figura 25, mostra da esquerda para direita, o processo onde uma figura seguida da mensagem a ser escondida resulta na figura final já estenografada, onde só seria detectada por uma análise minuciosa e através de programas específicos.

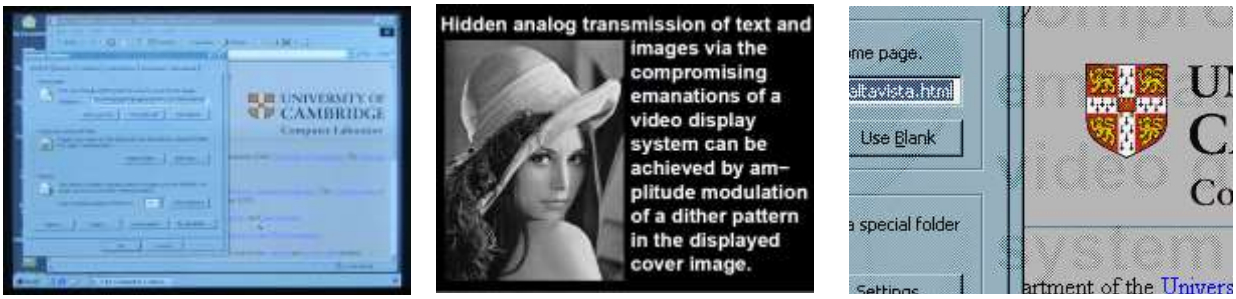


Figura 25 - Ilustrações sobre o processo de esteganografia.
Fonte: Kuhn, 2003.

Os pesquisadores sugerem algumas aplicações práticas para esse recurso: um programa capaz de controlar a emissão eletromagnética poderia ser usado como ataque, na forma de um código malicioso introduzido na máquina da vítima. A informação ou todo o conteúdo transmitido pelo cabo do monitor seria induzido a uma frequência conhecida pelo criminoso facilitando sua captação e burlando todo o sistema lógico e físico, já que ele estaria a certa distância do equipamento. Seria algo próximo do que fez Thiele escrevendo o *script* do programa *Tempest AM* de Riikonen e apresentado nos testes realizados no desenvolvimento (capítulo 3). De certa forma, bastaria alterar o *script* para coletar a informação desejada na máquina da vítima e não exibir a animação gráfica no monitor (figuras 15 e 19). Isto posto, passaria despercebido pela vítima e sistemas de segurança.

A esteganografia tem outra aplicação em um *software* patenteado por Kuhn e Anderson: *Soft Tempest* (1997). Este programa faz o mesmo que a aplicação anterior, mas

com o objetivo de detectar a instalação de *softwares* utilizados de forma ilegal (sem a compra da licença de uso). A empresa interessada incluiria o código em seu software para então ser comercializado e, com isso, teria o poder de realizar auditoria à distância sem o consentimento dos usuários, sendo clientes ou não, detectando se as licenças são válidas.

Contudo, a empresa poderia aplicar o código na forma de divulgação coletando dados da utilização de seu *software*: quando foi instalado, quantas horas por dia é usado, quais conexões com outros programas e quantas cópias foram distribuídas em determinada região. São recursos que dariam ideia do alcance do *software*, mas existem questões legais pertinentes de cada país para sua aplicação, pois a coleta de dados sem consentimento do usuário é habitual em vários *softwares*, páginas de *internet* e até sistemas operacionais.

5.4 Captação de sinais através de monitores

O projeto inicial desse trabalho de conclusão de curso estava focado em simular as experiências de van Eck (1985), um dos primeiros pesquisadores a publicar um experimento válido sobre a emissão eletromagnética de aparelhos eletrônicos, inclusive computadores. Sua técnica se baseia nos componentes internos de televisores e monitores de CRT, potentes geradores de campo eletromagnético, no qual idealizou um sintonizador apto a captar as mesmas frequências que os aparelhos emitem e assim reproduzir o conteúdo idêntico em seu sintonizador (figura 26). Ou seja, a tela do aparelho da vítima era praticamente clonada pelos equipamentos de van Eck, revelando tudo o que a vítima estava vendo, com a possibilidade de gravar seu conteúdo em videocassete. Isso quebra qualquer tipo de sistema de segurança ou criptografia já que é um processo externo ao computador.

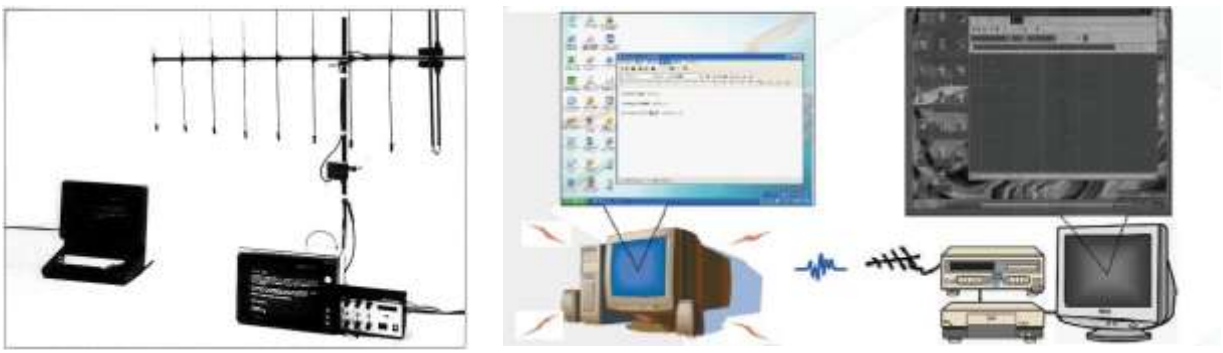


Figura 26 - À esquerda, fotografia do projeto original de van Eck em 1985. À direita, ilustração de como o sinal é captado. Fonte: VAN ECK (1985).

Após a publicação de van Eck, houve muita exploração do assunto em pesquisas científicas e reportagens pela imprensa mundial. Para exemplificar esse impacto, três vídeos

de reportagem mostram como o assunto foi divulgado: da BBC de Londres (BBC UK, [1985]), ainda nos anos 1980, destaca a vulnerabilidade no qual os bancos estavam expostos caso alguém utilizasse o método próximo à agência e uma improvável proteção metálica sugerida para evitar a emissão; da DTECH da Alemanha (DTECH GERMANY, 2007) abordando o método dentro de uma cabine blindada e com o *laptop* envolto em alumínio e ainda assim o sinal ainda é captado; da NHK do Japão (NHK JAPAN, 2010), a reportagem mais ampla apresentando os três métodos discutidos anteriormente (van Eck - monitor CRT; Kuhn - monitor LCD e cabos; Vuagnoux e Pasini - teclados) e outras vulnerabilidades, indicando algumas soluções como filtros atenuadores para cabos e blindagem de ambientes.

No Brasil, a matéria divulgada no jornal O Estado de S. Paulo em 1998 (SCAGLIA, 1998), com o título “Monitores jogam a criptografia pela janela” foi o núcleo de toda a pesquisa deste trabalho, discutindo abertamente sobre o *Tempest* e apontando diversas vulnerabilidades que expõem ambientes de trabalho das empresas aos criminosos (ANEXO).

Apesar da sugestão da matéria em recriar a experiência de van Eck, na prática, ficou inviável sua realização devido à dificuldade em encontrar conteúdo adequado e confiável. Foi preciso adaptá-lo para experimentos mais simples, como o *script* de Thiele que, apesar de simples, é o suficiente para comprovar a vulnerabilidade de sinais.

Certamente, os testes obtiveram êxito por empregarem tecnologias quase obsoletas. Com exceção do monitor LCD, fabricado em 2009, o computador e o *laptop* datam de 2004, equipados de conexão de vídeo VGA. E mesmo o monitor LCD do ambiente 1 sendo recente (conexão HDMI e compatibilidade HDCP), entrou de acordo com o que foi descrito por Kuhn (2011), a respeito da entrada VGA dos monitores, onde o sinal sofrerá conversão de digital para analógico permitindo a emissão eletromagnética. Para comprovar esse fato, observou-se que o monitor LCD do teste possui entradas para outras fontes de vídeo como RCA (videocassete), componente (DVD) e coaxial (antena). Ao ser alterada a seleção dessas entradas com o controle remoto durante o teste (PATRICIO, 2012), o som da emissão captado pelo aparelho de rádio não se alterou. Mas isso foi impugnado, pois ao desligar o monitor, o som da emissão continuou, provando que a emissão é causada pelo cabo e não pelo monitor.

Diferentes variações do ensaio e outros recursos são abordados no APÊNDICE A para o aprofundamento de novas pesquisas. Algumas propostas para reduzir a emissão eletromagnética de equipamentos são discutidas no APÊNDICE B.

6 CONCLUSÃO

A pesquisa aponta uma forma de invasão de sistemas praticamente desconhecida nos meios profissionais e sua simplicidade pode vir a causar danos financeiros irreparáveis caso alguma informação sigilosa, como um novo produto a ser lançado no mercado ou informação pessoal de clientes de uma empresa seja receptado por um concorrente.

Os resultados indicam, ainda, que toda a infraestrutura de uma organização composta de *firewalls*, antivírus, criptografia de dados, controle de acesso físico e lógico e políticas são passíveis de serem fraudadas, uma vez que ondas eletromagnéticas entram e saem dos equipamentos eletroeletrônicos, atravessam paredes e trafegam pelo ar sem que sejam notadas.

Globalmente, a área da informática tende a ser bem mais dinâmica em relação a outras, por sua constante evolução e mudança exponencial de tecnologia. A informática trouxe o progresso para as outras áreas como Ciência, Física, Engenharia, Medicina e tantas outras. Sem a informática, muitas profissões levariam tempo para efetuar cálculos complexos, fazer simulações em tempo real, criar estatísticas de mercado, previsões meteorológicas e trafegarem com informação em qualquer lugar do planeta.

Assim sendo, o profissional da área de segurança da informação deve empenhar todo conjunto de seu conhecimento em benefício da companhia para evitar que a informação fique exposta e crie meios para livrar as intrusões, por onde quer que elas se adentrem.

A atualização do aprendizado deve acompanhar a velocidade na qual a informática e todos os seus seguimentos avançam (APÊNDICE C). Para isso, o profissional precisa aplicar seu saber em especializações, palestras, cursos, participações em fóruns e eventos sobre o assunto e tudo mais que possa estar à frente dos criminosos, pois estes não seguem regras, padrões, leis e nem políticas de empresas. Por esse motivo, deve ir além de seu aprendizado para que na prática, saiba como o criminoso age e consiga encontrar soluções dinâmicas para os ataques.

Dessa forma, as discussões metodológicas apresentadas indicam que o domínio de mais uma camada relacionada à segurança é essencial para que o administrador de sistemas esteja atento às inúmeras possibilidades de invasão que podem comprometer a segurança da informação.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE COMPATIBILIDADE ELETROMAGNÉTICA - ABRICEM. ***Draft* da norma de exposição ambiental a campos magnéticos e elétricos - 60 Hz**. São Paulo: ABNT, 2000. 9 p. Disponível em: <http://www.abricem2.com.br/web3/pdfs/normas/60hz.pdf/>. Acesso em: 12 dez. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **ABNT ISO/IEC 17799:2005, Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 120 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **ABNT ISO/IEC 27001:2006, Sistema de gestão de segurança da informação – requisitos**. Rio de Janeiro: ABNT, 2006. 42 p.

ATHENIENSE, A. **O valor da política de segurança da informação na prevenção do vazamento de dados**. ASSESPRO-MG, 2012. Disponível em: <http://assespro.org.br/na-midia/noticias-regionais/2012-07-20-cafe-empresarial-da-assespro-mg-alertou-sobre-a-blindagem-da-empresa-para-evitar-o-vazamento-de-informacoes-e-a-perda-de-produtividade/>. Acesso em: 12 dez. 2012.

BALAN, W. C. **O espectro de frequência**. UNESP - curso de comunicação social, 1999. Disponível em: <http://www.willians.pro.br/frequencia/cap3_espectro.htm/>. Acesso em: 12 dez. 2012.

BBC UK. ***Van Eck Phreaking, a method of computer eavesdropping.*** [1985]. Disponível em: <https://www.youtube.com/watch?v=HYYm9Lin8X4/>. Acesso em: 12 dez. 2012.

BLACK BOX Corporation. ***Explains... tempest***. Pennsylvania, EUA. 2012. Disponível em: <http://www.blackbox.com/resources/blackboxexplains.aspx?id=BBE_4948/>. Acesso em: 12 dez. 2012.

BLACK BOX Corporation. ***Secure switching technology brief:*** *standards & clarification*. Pennsylvania, EUA. 2011. Disponível em: <http://www.blackbox.com/resource/genpdf/Buyers-Guides/TEMPEST-EAL4-BGUIDE.pdf/>. Acesso em: 12 dez. 2012.

BRAIN, M.; FENION, W. **Como funcionam os vírus de computador**. HowStuffWorks, 2011. Disponível em: <http://howstuffworks.com/virus2.htm/printable/>. Acesso em: 12 dez. 2012.

BRAIN, M. **Como funcionam as ondas de rádio**. HowStuffWorks, 2001. Disponível em: <http://informatica.hsw.uol.com.br/ondas-de-radio.htm/printable/>. Acesso em: 12 dez. 2012.

BRASIL. Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - INMETRO. **Grupo de trabalho compatibilidade eletromagnética**. Rio de Janeiro, RJ, 2007. 7 p. Disponível em: <http://www.inmetro.gov.br/qualidade/comites/atas/ata21ro_anexoI.pdf/>. Acesso em: 12 dez. 2012.

BRASIL. Decreto-lei nº 7.174, de 12 de maio de 2010. Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal. **Lex:** coletânea de legislação: edição federal, Brasília, DF, 2010. Suplemento.

BRASIL. Tribunal Superior Eleitoral. **Brasileiros já podem se inscrever para testar sistema eletrônico de votação**. Brasília, DF, 2009a. Disponível em: <http://agencia.tse.jus.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1221465&toAction=NOTI_VIEW_PORTAL&listState.itensPerPage=8/>. Acesso em: 12 dez. 2012.

BRASIL. Tribunal Superior Eleitoral. **Acompanhamento da execução do plano de teste**. Brasília, DF, 2009b, 7 p. Disponível em: <http://www.tse.gov.br/internet/eleicoes/arquivos/Teste_Sergio_Freitas.pdf/>. Acesso em: 12 dez. 2012.

BRASIL. Justiça Eleitoral Brasileira. **Testes de segurança mostram transparência do sistema eletrônico de votação**. Brasília, DF, 2012a. Disponível em: <http://www.youtube.com/watch?v=QPh7MdgYDb0&feature=share&list=SPAC6FA100EE88A1E1/>. Acesso em: 12 dez. 2012.

BRASIL. Tribunal Superior Eleitoral. **Testes de segurança:** investigadores têm acesso ao código-fonte da urna eletrônica. Brasília, DF, 2012b. Disponível em: <http://www.tse.jus.br/noticias-tse/2012/Marco/comeca-nesta-terca-20-2a-edicao-dos-testes-publicos-de-seguranca-na-urna-eletronica/?searchterm="testes publicos"/>. Acesso em: 12 dez. 2012.

BRASIL. Tribunal Superior Eleitoral. **Testes públicos de segurança do sistema eletrônico de votação**. Brasília, DF, 2012c. 22 p. Disponível em: <http://www.tse.jus.br/hotSites/testes-publicos-de-seguranca/index.html/>. Acesso em: 12 dez. 2012.

BRAUN, D. **Perito premiado esclarece teste de segurança com urna eletrônica**. Idg Now!, 2009. Disponível em: <http://idgnow.uol.com.br/seguranca/2009/11/24/perito-premiado-esclarece-teste-de-seguranca-com-urna-eletronica/>. Acesso em: 12 dez. 2012.

BUTCHER, G. ***National Aeronautics and Space Administration*** - **NASA:** *Tour of the electromagnetic spectrum*. NASA, EUA, 2010. Disponível em: <http://missionscience.nasa.gov/ems/TourOfEMS_Booklet_Print.pdf>. Acesso em: 12 dez. 2012.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em informática e de informação.** 3 ed. São Paulo: SENAC, 2006. 416 p.

CATÁLOGO BLACK BOX 2012 - **Referências técnicas**. São Paulo, 2012. 924 p. Disponível em: <http://www.blackbox.com.br/catalogoonline/>. Acesso em: 12 dez. 2012.

CC *by* 3.0. Licença Creative Commons para uso de obras. Califórnia, EUA, 2012. Disponível em: <http://creativecommons.org/licenses/by/3.0/deed.pt_BR/>. Acesso em: 12 dez. 2012.

CHIANENATO, I. **Gestão de pessoas:** e o novo papel dos recursos humanos nas organizações. 2 ed. Rio de Janeiro: Elsevier, 2005. 535 p.

CORTIZ, M. A. **Sigilo do voto com uso da urna eletrônica**. Rio Grande, 2010. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=7036&revista_caderno=28/>. Acesso em: 12 dez. 2012.

DANTAS, M. **Tecnologias de redes de comunicação e computadores**. Rio de Janeiro: Axcel Books, 2002. 327 p.

DEITEL & Associates Inc. ***Perl* -** como programar. Tradução por Pearson Education Inc. Porto Alegre: Bookman, 2002. p. 611.

DTECH GERMANY. ***Protecting computers from eavesdropping - Tempest***. 2007. Disponível em: <https://www.youtube.com/watch?v=vvOAIeVGRfw/>. Acesso em: 12 dez. 2012.

ESTADOS UNIDOS DA AMÉRICA. *National Security Agency.* ***History of communications security - COMSEC****.* Maryland, EUA, 1973. 94 p. Disponível em: <http://www.nsa.gov/public_info/_files/cryptologic_histories/history_comsec_ii.pdf/>. Acesso em: 12 dez. 2012.

ESTADOS UNIDOS DA AMÉRICA. *National Security Agency.* ***Tempest:*** *a signal problem.* Maryland, EUA, 1972. 5 p. Disponível em: <http://www.nsa.gov/public/pdf/tempest.pdf/>. Acesso em: 12 dez. 2012.

ESTADOS UNIDOS DA AMÉRICA. *US Air Force.* ***Air force systems security memorandum 7011****.* Washington D.C., EUA, 2009. 30 p. Disponível em: <http://www.altus.af.mil/shared/media/document/AFD-111108-040.pdf/>. Acesso em: 12 dez. 2012.

FELITTI, G. **Perito quebra sigilo e descobre voto de eleitores em urna eletrônica do Brasil**. Idg Now!, 2009. Disponível em: <http://idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/>. Acesso em: 12 dez. 2012.

GARLICK, D. ***TEMPEST and electromagnetic emanations security:*** *is not only a government standard.* The Sans Institute, Bethesda, MD, EUA, 2005. Disponível em: <http://www.giac.org/paper/gsec/4287/tempest-electromagnetic-emanations-security-government-standard/106943/>. Acesso em: 12 dez. 2012.

HEWITT, P. G. **Física conceitual**. 9 ed. Tradução por Pearson Education Inc. São Paulo: Bookman, 2002. p. 691.

IARRCIS EXI. Fotografia de Plousey Vincent. Dole, França, 2011. Disponível em: <http://tempest.hamradio.voila.net/ordinateuralanormetempest/image/sticker-tempest_big.JPG/>. Acesso em: 12 dez. 2012.

KELSEY, J. et al. *Side channel cryptanalysis of product ciphers*. **Journal of computer security**, San Jose, CA, EUA, v. 8, p. 141-158, 2000. Disponível em: <http://www.cs.berkeley.edu/~daw/papers/sidechan-final.ps>. Acesso em: 12 dez. 2012.

KOOPS, B. J. ***The crypto controversy:*** *a key conflict in the information society.* Dordrecht, Holanda: Kluwer Law International, 1999. 285 p.

KUHN, M. G. *Compromising emanations of LCD TV sets*. In: IEEE INTERNATIONAL SYMPOSIUM, 2011, Long Beach, CA, EUA. **Electromagnetic compatibility**: ISBN 978-1-4577-0811-4, p. 931–936. Disponível em: <http://www.cl.cam.ac.uk/˜mgk25/emc2011-tv.pdf/>. Acesso em: 12 dez. 2012.

KUHN, M. G. ***Compromising emanations:*** *eavesdropping risks of computer displays*. Reino Unido: University of Cambridge, Computer Laboratory, 2003. 167 p. Disponível em: <http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf/>. Acesso em: 12 dez. 2012.

KUHN, M. G.; ANDERSON, R. J. *Soft tempest: hidden data transmission using electromagnetic emanations*. In David Aucsmith (Ed.): INTERNATIONAL WORKSHOP, 2., 1998, Portland, Oregon, EUA. **Information hiding:** ISBN 3-540-65386-4, p. 124-142. Disponível em: <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf/>. Acesso em: 12 dez. 2012.

KUROSE, J. F.; ROSS, K. W. **Rede de computadores e a *internet*** - uma abordagem *top-down*. 3 ed. Tradução de Arlete Simille Marques. São Paulo: Pearson, 2006. 634 p.

MITNICK, K.; SIMON, W. L. **A arte de enganar**: controlando o fator humano na segurança da informação. Tradução de Kátia Aparecida Roque. São Paulo: Pearson, 2003. 284 p.

MODELO ATÔMICO ATUAL. Ilustração do Prof. Paulo César. 2010. Disponível em: <http://www.profpc.com.br/FIG8.JPG/>. Acesso em: 12 dez. 2012.

MORIMOTO, C. E. **Cabos de rede**. Guia do hardware. Rio Grande do Sul, 2008. Disponível em: <http://www.hardware.com.br/tutoriais/cabos-rede/>. Acesso em: 12 dez. 2012.

NHK JAPAN. ***Van Eck Phreaking Demonstration***. 2010. Disponível em: <https://www.youtube.com/watch?v=HjIhS_JQ80k/>. Acesso em: 12 dez. 2012.

OMOTE, N. **Física** - série sinopse. 3 ed. São Paulo: Moderna, 1982. p. 263-372.

PATRICIO, D. A. J. **Ambientes de teste**: experimento prático. Disponível em: <https://www.youtube.com/watch?v=RvYcV4fIxiE/>. Acesso em: 12 dez. 2012.

RIIKONEN, P. ***Tempest AM radio signal transmitter***. Finlândia, 2001. Disponível em: <http://xtrmntr.org/priikone/programs/tempest-AM-README/>. Acesso em: 12 dez. 2012.

SCAGLIA, A. Aparelho abre brecha para espionagem de PCs. **O Estado de S. Paulo**, São Paulo, 24 ago. 1998. Informática, Caderno G, ano 7, n. 356, p. 1; 3.

SINGEL, R. *Declassified NSA document reveals the secret history of TEMPEST*. **Wired Magazine**, San Francisco, CA, EUA, Abril, 2008. Disponível em: <http://www.wired.com/threatlevel/2008/04/nsa-releases-se/>. Acesso em: 12 dez. 2012.

SLAX: software livre. Versão 6.1.2. República Checa: Tomas Matejicek, 2009. Disponível em: <http://www.slax.org/>. Acesso em: 12 dez. 2012.

SOARES, E. **Nova urna eletrônica é mais segura**. Idg Now!, 2010. Disponível em: <http://idgnow.uol.com.br/ti-corporativa/2010/06/09/novas-urna-eletronica-e-mais-segura-diz-tse/>. Acesso em: 12 dez. 2012.

STALLINGS, W. **Criptografia e segurança de redes** - princípios e práticas. 4 ed. Tradução de Daniel Vieira. São Paulo: Pearson, 2008. 477 p.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Tradução de Vandenberg D. de Souza. Rio de Janeiro: Campus, 2003. 968 p.

TEMPEST FOR ELIZA: software livre. Versão 1.0.5. Alemanha: Erik Thiele, 2001. Disponível em: <http://www.erikyyy.de/tempest/tempest_for_eliza-1.0.5.tar.gz/>. Acesso em: 12 dez. 2012.

THE ELECTROMAGNETIC SPECTRUM. Ilustração de Advanced Photon Source - Argone National Laboratory. Lemont, IL, EUA, 2011. Disponível em: <http://farm7.staticflickr.com/6142/5940581568_1db150f055_b_d.jpg/>. Acesso em: 12 dez. 2012.

UNIVERSITY OF CAMBRIDGE. *Computer Laboratory*. Reino Unido. Markus Günther Kuhn, Ross John Anderson. ***Soft Tempest -*** *software piracy detector sensing electromagnetic computer emanations*. *UK Patent* GB2330924, 29 out. 1997, 06 ago. 2003 (application number GB9722799.5).

USENIX SECURITY SYMPOSIUM, 18., 2009, Toronto, Canadá. **Resumo...** Toronto, Canadá: Usenix, ISBN 978-1-931971-69-0. Disponível em: <http://www.usenix.org/events/sec09/tech/>. Acesso em: 12 dez. 2012.

VAN ECK, W. ***Electromagnetic radiation from video display units:*** *an eavesdropping risk?* Leidschendam, The Netherlands, 1985. 18 p. Disponível em: <http://cryptome.org/jya/emr.pdf>. Acesso em: 12 dez. 2012.

VUAGNOUX, M.; PASINI S. ***Compromising electromagnetic emanations of wired and wireless keyboards***. Lausanne, Suíça: LAboratoire de SÉcurité et de Cryptographie, 2008. Disponível em: <http://lasecwww.epfl.ch/keyboard/>. Acesso em: 12 dez. 2012.

VUAGNOUX, M.; PASINI S. *Compromising electromagnetic emanations of wired and wireless keyboards*. In: USENIX SECURITY SYMPOSIUM, 18., 2009, Toronto, Canadá. **Resumos...** Toronto, Canadá: ISBN 978-1-931971-69-0. Disponível em: <http://www.usenix.org/events/sec09/tech/full_papers/vuagnoux.pdf>. Acesso em: 12 dez. 2012.

WILSON, T. **Como funciona a HDMI**. HowStuffWorks, 2008. Disponível em: <http://eletronicos.hsw.uol.com.br/hdmi.htm/printable>. Acesso em: 12 dez. 2012.

APÊNDICE A - BASE DE APROFUNDAMENTO PARA NOVAS PESQUISAS

Os meses decorridos para elaboração deste trabalho de conclusão de curso apontou, durante o processo de pesquisa, diversos outros tópicos para o aprofundamento de novos trabalhos. A seguir, algumas propostas para averiguação:

Captura de sinais emitidos por monitores: diferente da emissão provinda de cabos, recriar linha a linha a imagem da tela da vítima requer conhecimento sobre o funcionamento interno de monitores. Técnicos de aparelhos de rádio e televisão podem auxiliar no desenvolvimento das simulações. Os métodos a serem explorados são de van Eck (monitor CRT) exposto no capítulo 2.4.4 e de Kuhn (*LCD* e *laptop*) no capítulo 2.4.5.

Captura de sinais emitidos por cabos de teclados: como apresentado no método de Vuagnoux e Pasini capítulo 2.4.6. Consiste em criar uma tabela relacionando as variações de frequência de cada tecla pressionada. Uma forma simplificada, como improvisou Silva com a urna eletrônica, seria usar somente os números do teclado, captar e gravar com um aparelho de rádio a frequência de cada tecla digitada, enviar para um programa que analise as formas de onda (como o *Audacity*) e montar a tabela correspondente às teclas.

Captura via conexão digital DVI / HDMI: método proposto por Kuhn em que avalia o protocolo TMDS para obter informações.

Captura indireta sem fio: tentativa de interceptar oscilações de frequências de dispositivos sem fio da mesma maneira descrito dos métodos com fio, ou seja, não capturar os dados transmitidos, mas variações de onda que possam ser interpretadas. Como exemplos, *internet* e rede sem fio (roteador *wireless*), *bluetooth*, telefone móvel (tecnologia 3G) e periféricos (teclado, *mouse*, impressora). Como a maioria destes dispositivos operam em média na faixa de 2,4 GHz, será preciso um receptor de satélite e antena parabólica.

Alterações no *script* de Thiele: fazer mudanças e ajustes, configurar ou compilar em formato MP3 outras músicas e pesquisar programas similares ao *Xvidtune*.

Captação de som de periféricos: várias pesquisas citam a interpretação de sons de equipamentos como modens analógicos, impressoras matriciais e até digitação no teclado.

Ataque com *mouse* modificado: a companhia de segurança Netragard (<http://www.netragard.com/>), especialista em testes de invasão, superou em 2011 o desafio em adentrar o sistema e o bloqueio de *firewall* a pedido de seu cliente utilizando engenharia social para presentear com *mouse* internamente alterado para invasão.

Ataque por canais laterais (*side-channel attacks*): a vulnerabilidade está no reflexo do brilho emitido pelo monitor nos mais diversos objetos como janelas, portas, paredes, jóias, garrafas, xícaras, caixas, CD, periféricos (especialmente com acabamento *black piano*), lentes de óculos e mesmo os olhos da vítima (KELSEY, 2000). Na Alemanha, o laboratório da Universidade de Saarland analisou um teste utilizando um mini telescópio e um *laptop* onde a tela apresentava um texto com fonte de tamanho 12. Mas o foco não era a tela e sim um bule de chá próximo ao *laptop* em que refletia o monitor e assim foi possível ler o texto completo a uma distância de dez metros. Com o auxílio de câmeras e lentes adaptadas é possível gravar os mínimos reflexos, mesmo distorcidos, e interpretá-los por meio de *softwares* que ampliam e recuperam a imagem gravada. De modo mais elaborado, consegue-se decifrar a leitura das luzes piscantes (*LED*) de equipamentos como modens, placas de rede e *switchs*.

Ataque *clickjacking*: com o domínio da câmera de vídeo (*webcam*) da vítima, um programa chamado *ClearShot*, capta a digitação do usuário interpreta tudo o que escreveu. Várias falhas de segurança em navegadores de *internet* com extensões instaladas (como Oracle *Java* e Adobe *Flash*) e mesmo anexos de mensagens e *links* de páginas na *internet* podem conter programas maliciosos que se instalam e obtém domínio da câmera. Esse assunto é estudado pelo pesquisador Giovanni Vigna, Ph.D em Ciência da Computação da Universidade da Califórnia em Santa Barbara, citando que o *ClearShot* possui vários algoritmos sendo aperfeiçoados para interpretar mais precisamente a digitação do usuário.

Na listagem de Referências há conteúdo amplo a ser explorado e muito desses documentos e páginas de *internet* possuem ligações para uma infinidade de outros estudos que podem servir de inspiração para outros trabalhos.

APÊNDICE B - PROPOSTAS PARA MINIMIZAR A EMISSÃO ELETROMAGNÉTICA

Com as lições aprendidas durante a pesquisa do trabalho, certas precauções para reduzir as possibilidades de emissão eletromagnética foram observadas e procurar compreender sua origem mostra ser o melhor caminho para amenizá-las. O eletromagnetismo é formado por campos elétricos e magnéticos (capítulo 2.4.1), sendo que cada campo gera interferências isoladamente e juntos precisam de soluções mais elaboradas para minimizá-las. Toda interferência existirá se houver três elementos: a fonte que emite a interferência, o receptor dessa emissão e o canal transmissor que liga os dois elementos. Se tomar como exemplo os itens empregados no desenvolvimento do capítulo 3, a fonte será o computador (ou cabo), o receptor correspondendo ao aparelho de rádio e o canal de ligação referindo-se ao próprio ar transportando a interferência.

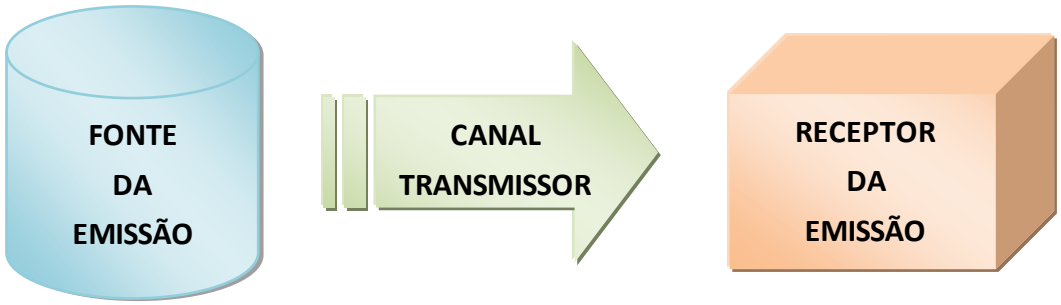


Figura 27 - Diagrama dos elementos responsáveis pela emissão.
Fonte: HEWITT (2002). Montagem própria.

A interferência elétrica é mais simples de se resolver quando conhecida sua causa e geralmente origina dos próprios componentes do equipamento ou de oscilações da rede elétrica. O ajuste da tensão elétrica com estabilizadores e o aterramento[19] de estacas de cobre no solo ligando todo circuito onde percorre a corrente elétrica são os procedimentos mais habituais, além de prevenirem acidentes com choque elétrico.

O campo magnético precisa de medidas mais aprimoradas como a blindagem envolvendo todo o equipamento e a anulação de fase, onde é gerada uma corrente elétrica idêntica a qual o campo magnético emite, mas com sua fase invertida, minimizando ou cancelando a emissão. Um exemplo desse uso é o cabo de par trançado. Na figura 28, à esquerda, observa-se os fios torcidos em pares, onde um dos fios transmite o sinal e seu par transmite o mesmo sinal com a fase invertida, como mostra o diagrama à direita. Em

[19] Sobre aterramento, o Brasil está imensamente atrasado nesse quesito impondo a norma ABNT NBR 14136 de 2010 com novo padrão de tomada com pino-terra, sendo que o padrão NEC desse tipo é obrigatório nos Estados Unidos desde 1913.

padrões mais rígidos desse cabo, como o CAT 7, cada par é envolto com folha de alumínio e todo o conjunto dentro da capa é coberto com malha metálica minimizando interferências.

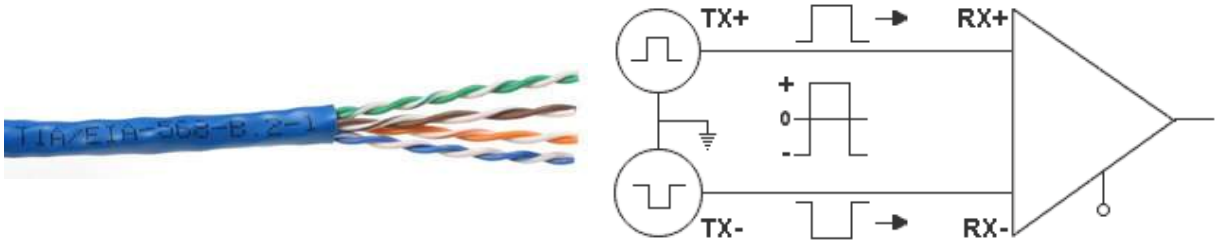


Figura 28 - Fotografia do cabo de par trançado e o diagrama de seu funcionamento.
Fonte: Morimoto, 2008.

Consequentemente, a interferência eletromagnética terá de empregar os métodos dos dois campos para que se possa atenuá-la. Isso requer estudo detalhado, medições dos campos e dependendo da dimensão do projeto a contratação de um profissional de engenharia. Algumas medidas básicas podem ser tomadas como:

- Consultar o manual de instruções: normalmente informam qual faixa de frequência opera o equipamento, as consequências do uso e como prevenir interferências.

- Procurar seguir as recomendações de procedimento das normas ABNT NBR 17799 e ABNT NBR 27001 e com elas criar a política de segurança interna da corporação.

- Pesquisar entre diversos fabricantes de filtros de emissão eletromagnética. A Quell (<http://www.eeseal.com/>) produz selos de silicone com microcomponentes embutidos (capacitores) que são acoplados nos conectores de equipamentos. A Laird Technologies (<http://www.lairdtech.com/>) fabrica espumas com propriedades especiais para absorver emissões. A empresa Vault (<http://www.vaultbr.com/>) oferece serviços de blindagem de equipamentos e ambientes especialmente em salas de informática e datacenter. Na página da ITEM (<http://www.interferencetechnology.com/category/digital-magazine/>) estão disponíveis guias de produtos e serviços de inúmeras empresas especializadas em tratar emissão eletromagnética.

- Se o setor da empresa exigir alta confidencialidade de informação adquirir equipamentos com certificação equivalente ao *Tempest*. No Brasil, como há pouca divulgação sobre o assunto, o número de empresas especializadas ou que comercializem produtos é escasso. A edição brasileira do catálogo Black Box menciona apenas três produtos descritos como 'Aprovação *Tempest*' e sugere entrar em contato com o suporte técnico para maiores esclarecimentos, enquanto que o catálogo americano é mais amplo, inclusive com soluções exclusivas para o Governo (*Federal It Solutions*).

- Usufruir de uma das aplicações do *SoftTempest* de Kuhn e Anderson (capítulo 2.4.5), já que eles mesmos constataram a dificuldade em evitar a emissão eletromagnética, então o programa cria uma distorção no texto apresentado no monitor mantendo-o legível ao usuário, mas indistinguível se for captado por emissão. Na figura 29 à esquerda, os quadros mostram o processo de distorção ajustado até limite no qual se consegue ler e à direita a simulação de como fica o imagem do monitor do usuário ao lado de como estaria se fosse captado por emissão. Esse efeito é basicamente o contrário do ajuste *ClearType*, nativo do sistema operacional Microsoft Windows XP e posteriores, e seu propósito é deixar o texto mais nítido. Desse modo, se necessária a privacidade dos dados, seria conveniente desabilitar esse recurso.

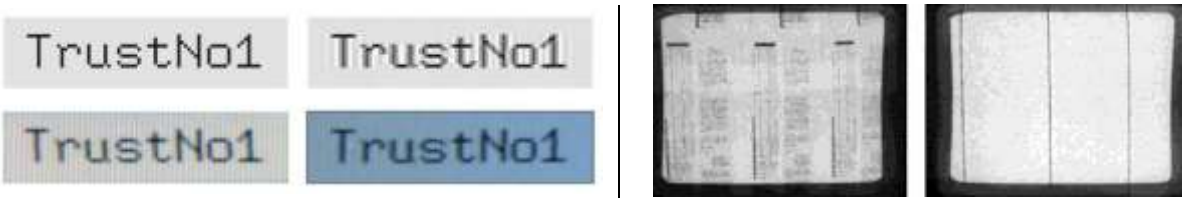


Figura 29 - Ilustrações do modo em que o *SoftTempest* distorce a informação no monitor.
Fonte: Kuhn, 1998.

- Aproveitando a solução do *software* de Kuhn, um artifício para criar ruído na conexão entre a placa de vídeo com o monitor também dificultaria a interpretação pelo criminoso. Para isso, o ruído deveria ser aleatório para que nenhum programa possa interpretar seu algoritmo.

APÊNDICE C - O QUE ESPERAR DA SEGURANÇA DA INFORMAÇÃO?

A tecnologia é fator imprevisível pelos cientistas em meio a tantas descobertas exploradas devido ao próprio avanço da informação e o progresso acaba por encurtar a vida de invenções que mal foram exploradas. O telefone móvel é uma amostra da velocidade de como a tecnologia traz avanços e, da mesma forma, aposenta de maneira precoce produtos recém-lançados. Como já citado, a informática trouxe o avanço necessário para que outras profissões evoluíssem e a segurança da informação tem a responsabilidade de antever a ação de criminosos em razão de a tendência apontar para que todos os equipamentos conhecidos estejam interconectados, principalmente os mais usuais como o televisor. Assim, alguns itens a seguir, tendem a aperfeiçoar a segurança dos dispositivos futuros:

Criptografia quântica: diferente da criptografia tradicional feita por *bits*, os fótons (capítulo 2.4.1) são empregados para criar algoritmos mais sofisticados e seguros na distribuição de chaves (TANENBAUM, 2003).

Fibra óptica plástica: é incontestável a vantagem da fibra óptica em relação ao cabo comum de cobre, como não irradiar emissões eletromagnéticas, velocidade superior de transmissão, imunidade à corrosão e diversos outros fatores. Mas, os equipamentos responsáveis por sua transmissão são relativamente caros. Pesquisas com materiais como o plástico para a fabricação das fibras e equipamentos mais simplificados devem permitir que a tecnologia se torne mais acessível.

Tela sensível ao toque: sugerida por Canut (capítulo 2.4.6), vem como alternativa ao teclado dispensando o uso de cabos já que é embutido no monitor.

Teclado projetado a laser: produz total ou parcialmente o teclado em qualquer superfície rígida e transmite via *bluetooth* ao computador.

Conexões de vídeo integralmente digitais: com o fim decretado do padrão VGA pelos fabricantes em 2015, após quase 30 anos de seu lançamento, os monitores e placas de vídeo não necessitarão mais de conversores analógico-digitais que encarecem e tornam as conexões vulneráveis (capítulo 4).

Protocolo HDCP em computadores: o emprego desse protocolo para proteção de obras com direito autoral (capítulo 4), poderia se estender nas conexões de vídeo de informática para melhorar a confidencialidade de sinais emitidos.

APÊNDICE D - EMISSÃO ELETROMAGNÉTICA E SAÚDE

Da mesma forma que a tecnologia trouxe benefícios e tornou a vida dos seres humanos mais cômoda, também acarretou diversos efeitos colaterais em vários aspectos. A emissão eletromagnética de equipamentos, além do problema em deixar transportar informação de dados, pode apresentar quadros de doenças aos seres vivos dependendo da distância e tempo de exposição. A falta de conhecimento da população, por vezes omitido pelos próprios fabricantes de equipamentos e outros seguimentos de empresa, acarreta prejuízos na saúde em longo prazo, visto que, certas radiações surgem depois de anos de exposição. O telefone móvel divide opiniões quanto ao seu uso, mas é certo que o período prolongado pode trazer sequelas. O forno de micro-ondas se comprado com problemas de fabricação ou estiver desregulado emite radiações além do permitido. Morar próximo a estações de energia, antenas transmissoras e de telefonia móvel, transformadores de postes, entre outros, são assuntos tratados por entidades do Governo, como a ABRICEM e CBAC, (capítulo 2.4.3) com o termo "Compatibilidade Eletromagnética" e visam criar regulamentações e normas (ABNT / NBR) já que o país ainda não tem certificação.

Algumas associações discutem o assunto em forma de palestras, seminários e páginas na *internet*, como a PoaVive[20] que ministrou o seminários sobre emissões eletromagnéticas não ionizantes (figura 30).

Uma explanação sintetizada sobre radiação e saúde pode ser conferida na página da empresa ProRad, disponível em <http://www.prorad.com.br/cursos/Cursos/rni.pdf>.

Figura 30 - Ilustrações sobre o efeito das emissões eletromagnéticas à saúde.
Fonte: Diversas com licença CC 3.0.

[20] A página está disponível em: <http://poavive.wordpress.com/2012/12/23/carta-do-seminario-sobre-os-riscos-da-radiacao-eletromagnetica-nao-ionizante-da-telefonia-celular/>

ANEXO - ÍNTEGRA DA MATÉRIA DE ALEXANDRE SCAGLIA

Aparelho abre brecha para espionagem de PCs

Tempest custa US$800 na Internet e pode capturar emissões de monitor a 1 Km

Quando ficou definido que o presidente norte-americano Bill Clinton iria dar seu depoimento sobre seu envolvimento com a ex-estagiária da Casa Branca Mônica Lewinsky por uma rede de vídeoconferência, a comunidade de hackers ficou em polvorosa. Afinal, aparecer no circuito mundial seria uma glória.

Para evitar que isso acontecesse, foi criada uma ligação direta entre a Casa Branca (onde estaria Clinton) e o tribunal, usando cabos de fibra ótica. Além disso, a transmissão seria criptografada. Até esse ponto, nenhuma novidade em termos de segurança.

Mas um pequeno detalhe poderia pôr a perder toda a estrutura montada: os aparelhos de TV. Uma tecnologia conhecida como Tempest permite que se copie as imagens ou textos diretamente da tela de um monitor de computador ou aparelho de TV. Para evitar esse tipo de problema, o depoimento foi visto pelos jurados do caso em um aparelho especialmente blindado, que impede a captação das ondas emitidas pelos eletrodomésticos.

"Equipamentos usando a tecnologia Tempest podem ser construídos em casa por qualquer pessoa com um pouco de conhecimento de funcionamento de uma televisão", garante KingPin, um hacker consultado sobre o tema pela Casa Branca.

Além de poder ser construído por pessoas com conhecimento em eletrônica, a Internet é fonte de diversos guias de funcionamento e montagem. No endereço **http://www.cftecodes.com** é possível até comprar uma solução Tempest completa.

Monitor do sistema (acima) e tela vista pelo espião (abaixo)

Como funciona: o receptor direcional capta a radiofreqüência emitida pelo monitor. O Tempest reconstrói a imagem em outro monitor

CLINTON FEZ DEPOIMENTO EM MONITOR BLINDADO

Falhas de segurança – Outros problemas que têm comprometido a tranquilidade de quem navega na Internet são as falhas outras mais populares programas de e-mail e o lançamento de um software específico para invadir computadores rodando Windows 95 e 98, o Back Orifice, que abre uma porta de acesso sem que o usuário da máquina perceba o que está acontecendo. Página 3

Monitores jogam criptografia pela janela

Uma simples antena adaptada é capaz de copiar tudo o que é mostrado na tela

ALEXANDRE SCAGLIA

Sofisticadas chaves de criptografia, firewalls e outras formas de garantir a segurança dos dados transmitidos ou arquivados eletronicamente podem não valer nada. Tudo porque os monitores estão vulneráveis a uma forma nesse tão refinada de invasão, a cópia.

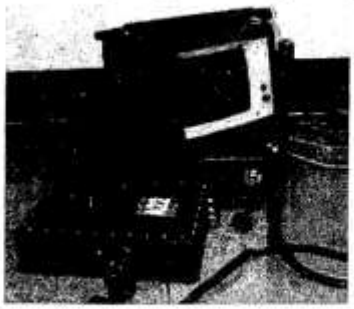
Usando uma antena e um equipamento corretamente montado, qualquer pessoa, mesmo a centenas de metros de distância, pode ver o que está sendo escrito, lido ou visto em um monitor ou aparelho de TV.

Conhecida como Tempest, essa técnica de monitoração foi descoberta em 1985 por um cientista holandês chamado Wim van Eck, que publicou um estudo a respeito do tema. Eck baseia-se no fato de que os monitores e aparelhos de TV criam a imagem pela varredura de um feixe de elétrons que percorre a tela de um lado para outro rapidamente.

O que um equipamento Tempest faz é sintonizar a freqüência da onda criada na varredura e reconstruí-la a distância. Além da facilidade de ser um problema para o qual quase ninguém presta atenção, cabos não-blindados em geral (de telefone, impressoras e etc.) funcionam como uma antena, aumentando ainda mais o alcance das ondas.

Prova de que tal vulnerabilidade não é levada a sério é que, em recente depoimento ao senado americano, o hacker KingPin, integrante do grupo americano L0pht, foi brevemente questionado sobre o assunto. "Os responsáveis pela seção não deram muito foco em falhas de segurança eletrônica e de hardware", afirma. "Bom para mim e ruim para eles, que continuam se arriscando."

KingPin garante que qualquer pessoa com um razoável conhecimento em tecnologia televisiva consegue fazer um equipamento Tempest. "Depois, basta apontar a antena e copiar o arquivo criptografado."



Exemplo de solução Tempest: monitor é usado para reproduzir a distante tela capturada pela antena e receptor, enquanto dados da varredura são gravados para posterior análise

Figura 31 - Reprodução do encarte de jornal com a matéria sobre o *Tempest* (adaptado). Fonte: Agência Estado (SCAGLIA, 1998).