DESENVOLVIMENTO DE UM *NVR* PORTÁTIL PARA UTILIZAÇÃO EM CÂMERAS DE VIGILÂNCIA *IP*

IVAN CÉSAR OLIVEIRA MURÇA [1]
CLAYTON EDUARDO DOS SANTOS [2]

RESUMO

O advento da *Internet* e a popularização dos *smartphones* destacam-se como peças fundamentais no processo de inclusão digital de um número expressivo de pessoas, de diferentes idades e classes sociais, ao redor do mundo. Dessa forma, o dispositivo que na visão de grande parte desse público, a princípio, seria utilizado única e exclusivamente para realizar ligações telefônicas, se transformou em uma ferramenta de comunicação, trabalho e lazer sem precedentes, passando a desempenhar papel determinante no cotidiano das pessoas. Sendo assim, é natural que novos produtos e funcionalidades, outrora tidos como futuristas, passassem a fazer parte do portfólio de serviços disponíveis nas plataformas móveis. Os dispositivos inteligentes, voltados a automação residencial e comercial, tem sido a grande vedete dessa nova onda e o termo *IoT*, tem estado a cada dia mais presente no vocabulário do grande público. Dentre as funções oferecidas por tais dispositivos, destacam-se especialmente as voltadas à segurança patrimonial, sobretudo as câmeras *IP*. É possível, a partir de um simples *smartphone*, monitorar ambientes remotos com qualidade de imagem e som. No entanto, o conforto proporcionado por tal solução é atraente em termos de funcionalidade, mas nem sempre no fator custo. Dessa forma, dispositivos genéricos, com segurança questionável e por vezes sem suporte ou atualizações, correspondem a grande maioria da base instalada. Disponibilizar um dispositivo portátil, capaz de mitigar as principais vulnerabilidades presentes no cenário supracitado, é o objetivo do presente trabalho.

Palavras-chave: Câmera *IP*, Código Aberto, Dispositivos Embarcados, *FreeBSD*, Monitoramento, *NVR*, *Raspberry Pi*, *IoT,* Segurança da Informação.

[1] Pós-graduando em Gestão Estratégica de Tecnologia da Informação pelo Instituto Federal de São Paulo - Campus de Bragança Paulista – e-mail: *ivan.murca@gmail.com.*
[2] Professor Doutor do Instituto Federal de São Paulo – Campus de Bragança Paulista – e-mail: *claytones@ifsp.edu.br.*

DEVELOPMENT OF A PORTABLE NVR FOR USE IN IP SURVEILLANCE CAMERAS

ABSTRACT

The advent of the Internet and the popularization of smartphones stand out as key pieces in the process of digital inclusion of a significant number of people of different ages and social classes around the world. The device that, at first, would be used exclusively to make telephone calls, has become an unprecedented tool of communication, work and leisure, playing a determining role in people's daily lives. Thus, it is natural that new products and features, once considered futuristic, would become part of the portfolio of services available on mobile platforms. Intelligent devices, aimed at home and commercial automation, have been the star of this new wave and the term IoT has been increasingly present in the vocabulary of the general public. Among the functions offered by such devices, those focused property security, especially IP cameras. A simple smartphone is capable of monitoring remote environments with picture and sound quality. However, the comfort provided by such a solution is attractive in functionality, but not always in the cost factor. Thus, generic devices with questionable security and sometimes no support or upgrades correspond to the vast majority of the installed base. Providing a portable device capable of mitigating the main vulnerabilities present in the above scenario is the objective of the present work.

Keywords: *IP Camera, Open Source, Embedded Devices, FreeBSD, Monitoring, NVR, Raspberry Pi, IoT, Information Security*

1 - INTRODUÇÃO

Dentre as inúmeras contribuições que a computação disponibiliza a seus usuários, não poderíamos deixar de destacar duas em especial: a possibilidade de confecção de soluções criativas para os mais diversos problemas e a automatização de processos. Atualmente, tecnologias que até pouco tempo atrás eram tidas como promessas ou até mesmo devaneios provenientes de obras de ficção científica, tem se tornado parte do cotidiano dos mais diversos públicos. Alguns exemplos que podem ser citados nesse aspecto são os comunicadores portáteis, as vídeo chamadas e mais recentemente, os dispositivos inteligentes controlados por voz. Tais tecnologias tiveram um longo processo de elaboração, criação e amadurecimento até que efetivamente pudessem chegar ao grande público. Atualmente, as tecnologias supracitadas podem ser facilmente associadas aos *smartphones* e às casas inteligentes, tendo em vista a familiaridade da população em geral com os referidos temas, mas nem sempre foi assim. Evidentemente que, como em qualquer tecnologia de vanguarda, consumir serviços de ponta tem seu custo. O processo de popularização de tecnologias e dispositivos é lento, tendo em vista seu alto custo inicial, de aquisição e manutenção, bem como o direcionamento às camadas de maior poder aquisitivo da sociedade. Com o passar do tempo, o público alvo dos fabricantes passa a ser mais amplo, abrangendo inclusive os chamados países emergentes e a população de modo geral. Dessa forma, os requisitos funcionais dos dispositivos tendem a se tornar mais flexíveis, em função do menor grau de exigência praticado por grande parte da população, de seu poder de compra reduzido e em especial, da limitação do conhecimento técnico. Com isso, os dispositivos se tornam mais acessíveis, tendo em vista a diminuição dos custos de produção que acabam por refletir no valor praticado na venda e por consequência na manutenção dos serviços agregados, A pergunta é: a que preço? Fatores como qualidade, performance e sobretudo segurança, fatalmente são negligenciados nessa expansão de mercado.

1.1 - MOTIVAÇÃO

Com o surgimento da banda larga e a inclusão digital promovida pelos dispositivos móveis, em especial os *smartphones*, um novo mundo de oportunidades passou a fazer parte do universo do consumidor atento ao mercado de tecnologia, atualmente presente em todas as camadas da população. Ao se habituar com o oferecimento e consumo de bens e serviços em uma nova plataforma, o cidadão comum, de maneira geral, passou a adotar os aplicativos móveis como principal instrumento de comunicação e interação, deixando de lado tecnologias que dominaram esse terreno por décadas, como por exemplo, o telefone fixo e demais serviços associados. A informação a um clique, a interface intuitiva e o dinamismo oferecido pelos aplicativos móveis transformaram usuários leigos em fiéis seguidores desse novo paradigma, em especial graças aos comunicadores instantâneos e às redes sociais. Mais recentemente, a chamada "*Internet* das Coisas", tem chamado a atenção do grande público em especial, por oferecer recursos e dispositivos que até então eram considerados distantes da realidade de grande parte da população. Os dispositivos embarcados e as funcionalidades oferecidas nas casas inteligentes permitiram que funcionalidades significativas de automação fossem incorporadas a interface de aplicativos móveis trazendo recursos voltados à segurança e monitoramento patrimonial para o cotidiano do usuário comum. Dessa forma, dispositivos como câmeras *IP*, permitem que o cidadão monitore a área interna e externa da sua casa ou comércio, eventualmente grave imagens e vídeos em um sistema de gravação dedicado, normalmente um *DVR* ou *NVR*, e até mesmo acompanhe essa rotina pelo celular, de onde estiver. Evidente que se tratam de recursos inovadores e sedutores, tanto do ponto de vista funcional como econômico, tendo em vista o oferecimento de equipamentos com opções voltadas para todos os bolsos, em especial, graças aos produtos de entrada produzidos na China e facilmente encontrados localmente no país desde lojas físicas especializadas ou principalmente via comércio eletrônico na *Internet*.

1.2 - JUSTIFICATIVA

Tendo em vista o exposto, não são raros os incidentes de segurança envolvendo os chamados “dispositivos inteligentes”, atualmente tão comuns no cotidiano das pessoas. Dispositivos de rede de maneira geral, oferecem “parâmetros padrão” definidos pelo fabricante para a configuração inicial dos dispositivos, de modo a facilitar a instalação e operação por parte dos usuários finais, bem como diminuir o número de chamados destinados ao setor de suporte. Os parâmetros envolvidos nessa pré-configuração invariavelmente estão relacionados com o endereço de rede e com os dados de autenticação do usuário, fatores sensíveis que deveriam ser modificados pelo usuário após a configuração inicial do dispositivo, o que muitas vezes não acontece. Os equipamentos com maior incidência desse tipo de problema são os relacionados à conectividade e monitoramento, em especial, roteadores, *modems*, pontos de acesso, *DVRs*[3], *NVRs*[4] e câmeras *IP*. Aliado a essa questão, temos também os fabricantes *OEM*[5] que fornecem os equipamentos a distribuidores que, por sua vez, colocam sua marca e revendem o produto o que, em grande parte dos casos, implica em dispositivos de baixo custo, com diversas vulnerabilidades que em geral não recebem atualizações de *firmware*, comprometendo dessa forma, a segurança, funcionalidade e até mesmo a viabilidade da manutenção do equipamento em ambiente de produção.

1.3 - OBJETIVO

O objetivo do presente trabalho é implementar um dispositivo portátil que atue como elemento concentrador capaz de gerenciar câmeras *IP* individualmente ou em quantidade, oferecendo acesso às imagens disponibilizadas por tais dispositivos sem os riscos de segurança normalmente encontrados em equipamentos diretamente

[3] *DVR (Digital Video Recorder)* é um dispositivo eletrônico que permite monitorar, gerenciar e armazenar imagens em formatos digitais a partir de câmeras com sinais analógicos.
[4] *NVR (Network Video Recorder)* é similar ao *DVR* quanto a funcionalidade, porém difere-se dos tipos de câmeras das quais são capturadas as imagens, pois operam somente com câmeras que usam protocolo *TCP-IP*.
[5] *OEM (Original Equipment Manufacturer),* ou seja, fabricante de produtos ou componentes originais que são vendidos sob a marca de outra organização empresarial que encomendou seu *design* e fabricação (SAAVEDRA *et al.,*2013).

conectados à *Internet,* sejam eles câmeras, *DVRs* ou *NVRs* de entrada utilizados em massa no mercado.

2 - REVISÃO BIBLIOGRÁFICA

Nessa seção serão abordados temas e tecnologias relevantes e correlatos com o propósito da presente pesquisa.

2.1 - A INTERNET DAS COISAS

A nomenclatura *Internet of Things (IoT*, Internet das Coisas) foi criada em 1999 por Kevin Ashton um pesquisador do Instituto de Tecnologia de Massachusetts (*MIT*) *Auto-ID Laboratory*, em uma demonstração sobre identificação por rádio frequência (*RFID*) na cadeia de suprimentos de uma grande corporação. (ASHTON, 2009).

Essa nova tecnologia, tem sido alavancada pelas redes móveis e a *Internet*. De acordo com a ITU (2005), as redes *IoT* do futuro serão capazes de detectar e monitorar em tempo real as mudanças no estado físico de dispositivos interligados em rede.

Para Atzori (2011), a IoT é a presença distribuída de vários objetos ou dispositivos, com endereços únicos (câmeras *IP*, *smartphones, tablets, RFID*, sensores, entre outros) que podem interagir entre si e cooperar para alcançar objetivos comuns.

A *IoT* consiste em protocolos e tecnologias relacionadas que permitem que elementos diferentes se conectem através de canais de comunicações eletrônicas, com ou sem fio, numa rede de troca de dados e informações compostas por coisas e pessoas (VALÉRY, 2012). Segundo Marotta (2013), com a *IoT* nasceu o conceito de dispositivos inteligentes, e esses dispositivos podem interagir com os componentes de rede já existentes, como roteadores, *switches, gateways*, dentre outros.

Ao analisar os conceitos anteriormente mencionados, é possível concluir que a *Internet* das Coisas é uma extensão da *Internet* atual, que permite aos objetos cotidianos com capacidade computacional e de comunicação, conectarem-se à *Internet*. A conexão com a rede mundial de computadores viabiliza controlar remotamente os objetos e permitir que os próprios objetos sejam acessados como provedores de

serviços. Essas novas habilidades em objetos comuns, geram um grande número de oportunidades em diversos segmentos, tais como: a indústria, o comércio, a saúde a educação e outros. Porém, estas possibilidades apresentam riscos e acarretam grandes desafios técnicos e sociais as comunidades.

2.2 - DISPOSITIVOS INTELIGENTES

O conceito de “dispositivos inteligentes” começou a ser forjado no início dos anos 90 numa visão futurista do criador da computação ubíqua, Mark D. Weiser (1991), que fez vários estudos se utilizando de *palmtops*, *laptops* e computadores conectados em uma rede sem fio. Naquela época ele já imaginava uma grande rede onipresente, na qual diversos dispositivos poderiam se conectar, interagir entre si e com os seres humanos. Previu requisitos necessários para escalabilidade e disponibilidades dos serviços.

Um dispositivo inteligente, é um dispositivo eletrônico dotado de alguma capacidade computacional e de um sistema de comunicação, que geralmente esta conectado a outros dispositivos ou redes de computadores por meio de diferentes protocolos de comunicação com ou sem fio (*TCP IP, Bluetooth, Wi-Fi, NFC, Zigbee, 4G, 6LoWPAN* e etc), que funcionam de forma interativa e que por vezes operaram de forma autônoma. Exemplos de dispositivos inteligentes: *smartphones*, *smartwatches*, *tablets*, câmeras *IPs*, fechaduras eletrônicas inteligentes dentre outros.

2.3 - AMEAÇA

Uma ameaça pode ser identificada como um conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em danos para um sistema ou organização (Departamento de Informática do Sistema Único de Saúde-DATASUS, 2015).

Para Sêmola (2003), ameaças são os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas.

As ameaças são classificadas em: desastres naturais (enchentes, incêndio, terremoto), humanas (subdividida em intencional, onde ocorre diretamente por hackers e funcionários descontentes e não intencional, onde funcionários com pouco conhecimento sobre a tecnologia aplicada) e ambientais (engloba toda parte tecnológica, software, hardware, falhas de sistema operacional, falha elétrica) (SIMÕES, 2014).

2.4 - *MALWARE*

O *malware* é um programa que discretamente se instala num sistema de processamento de dados, sem o conhecimento ou consentimento do usuário, com o objetivo de colocar em perigo a confidencialidade e integridade dos dados ou a disponibilidade do sistema (FILIOL, 2005).

Abaixo listamos algumas das diversas formas como os códigos maliciosos podem infectar computadores ou sistemas informatizados:

- Por meio de vulnerabilidades existentes em programas instalados;
- Autoexecução de mídias removíveis infectadas, como *DVDs* e *pendrives*;
- Atacantes que invadem o computador infectando-o com códigos maliciosos;
- Acesso a páginas *Web* com conteúdos maliciosos, utilizando-se de navegadores vulneráveis ou desatualizados;
- Pela execução de arquivos previamente infectados, como anexos de mensagens eletrônicas ou de outros computadores (através do compartilhamento de recursos).

2.4.1 - VÍRUS

O vírus é um tipo de *malware* concebido para se replicar e espalhar no sistema informático, podendo danificar o sistema, eliminar dados, e desativar programas de segurança (por exemplo antivírus) (ERBSCHLEO, 2005).

Segundo Boltd (2010), o vírus em regra, necessita da interação humana para se propagar, particularmente através de utilização de um *CD/DVD-ROM* ou dispositivos *USB*, ao contrário de variantes similares aos vírus, em especial no que se refere a seus efeitos práticos, porém com propagação via *Internet*, não dependendo dessa forma, da interação humana.

2.4.2- *WORMS*

Worms são um tipo praga virtual, que tem como característica principal a autoduplicação, não necessitando portanto, de programas como vetor de contaminação, pois residem e se multiplicam em ambientes multitarefa e exploram vulnerabilidades para que possam executar processos remotos em sistemas distribuídos.

Conforme a *Panda Security* (2018), o objetivo dos *worms* é se espalhar infectando o maior número de dispositivos, por meio da técnica de multiplicação, que consiste na criação de diversas cópias de si mesmo que em seguida, são propagadas via e-mails, mensagens de texto, ou alguma outra forma de conexão entre usuários.

2.4.3- *SPYWARE*

Os *spywares* são *malwares* que tem como objetivo monitorar as atividades realizadas em dispositivos computacionais. Ele coleta as informações sobre os hábitos *online*, históricos de navegação ou dados pessoais (como número do cartão de crédito e senhas) e envia tais informações a terceiros (CERT, 2017). Alguns tipos específicos de *spyware* são:

- ***Keylogger*:** captura e armazena as teclas digitadas pelo usuário sendo ativado normalmente, quando ocorre um acesso específico de comércio eletrônico ou de *Internet banking*.
- ***Screenlogger*:** semelhante ao *keylogger*, armazena a posição do cursor e a tela visualizada no monitor, nos momentos em que o *mouse* é clicado. Bem

utilizado pelos atacantes, para capturar teclas clicadas em teclados virtuais pelo usuário.

- ***Adware*:** concebido para apresentar mensagens publicitárias em navegações realizadas pelo usuário. Tem uso legal quando incorporado a programas ou serviços de patrocínio remunerado. Porém, pode ser utilizado para fins maliciosos, no momento em que as propagandas são direcionadas, conforme a navegação do usuário sem que ele tenha conhecimento do monitoramento que está sendo realizado.

2.4.4 - *BOTS E BOTNETS*

Bots são programas que procuram por vulnerabilidades e falhas de *softwares* instalados em dispositivos computacionais, a fim de explorá-las remotamente tornando-o um dispositivo zumbi. *Bot*, também conhecido como robô, recebe este nome, pois é programado para agir como tal, quando ativado de forma remota pelo invasor.

Ainda segundo a cartilha de segurança do CERT (2017), *bot* é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente explorando vulnerabilidades existentes em programas instalados em computadores e afins

Botnet é uma rede que pode ser composta por centenas, milhares talvez milhões de dispositivos zumbis infectados por *bots*, que permitem potencializar ações danosas em uma ou várias redes de computadores. Algumas das ações maliciosas executadas por intermédio de *botnets* são: a propagação de códigos maliciosos, coleta de informações de inúmeros dispositivos computacionais, ataques de negação de serviço, envio de spams e camuflagem da identidade do atacante (CERT, 2017).

Nesse mesmo contexto, Puri (2003, p.10) corrobora que:

> *Botnet* ou o exército de *bots* de alta velocidade podem ser efetivamente usados para manter discretamente a capacidade do ataque *DDoS* de alto valor e para lançar ataques de rede coordenados em qualquer momento desejado, conforme indicado pelo mestre de controle por meio do invasor.

Basicamente o funcionamento de um ataque por *botnet* passa pelas seguintes etapas, o atacante propaga um determinado tipo de *bot*, geralmente incorporado a outro arquivo na tentativa de infectar o maior número possível de dispositivos computacionais, os computadores infectados passam a ficar a disposição do atacante que assume o controle dos *bots* através de uma central de controle e comando.

Quando o *botmaster*, entidade externa que coordena as ações dos *bots*, deseja que uma ação seja realizada, ele envia os comandos a serem executados, por meio de redes do tipo *P2P* ou servidores centralizados, os computadores zumbis executam os comandos recebidos e agem pelo tempo determinado pelo *botmaster*. Ao finalizarem a ação, os zumbis retornam ao modo de espera e ficam no aguardo dos próximos comandos a serem executados (PAUL BÄCHER *et al*, 2004).

2.4.5 - BACKDOOR

O *backdoor* tem o objetivo de anular uma autenticação necessária para acessar um dispositivo ou sistema. Por vezes combinado com a engenharia social, estuda-se uma eventual vítima com intuito de obter suas credenciais de *login*, de posse de tais informações o atacante poderá acessar remotamente o sistema ou dispositivo e executar comandos sem que a vítima perceba. Há pouco tempo, *backdoors* foram descobertos em inúmeros dispositivos utilizados na *Internet* das Coisas, como câmeras *Wi-Fi* usadas em residências e organizações. Uma vez infectado, o dispositivo *IoT* é transformado em um zumbi acessível via *backdooor*, permitindo dessa forma que acessos sejam feitos sem os procedimentos padrão de autenticação (INCAPSULA, 2017).

2.4.6 - *ROOTKIT*

Rootkit é um tipo de *malware* concebido com o objetivo de auferir privilégios administrativos, por meio de programas e técnicas que permitem esconder e assegurar a presença de um atacante ou outro código malicioso (CERT, 2017). O seu uso possibilita, remover rastros em arquivos de *log*, instalar *backdoors* e assim assegurar o

acesso futuro em máquinas infectadas, ocultar atividades e informações referentes a arquivos, chaves de registro, diretórios, processos e etc. Assim como, mapear potenciais vulnerabilidades em outros dispositivos conectados a rede, através de varreduras na rede.

2.5 INCIDENTES DE SEGURANÇA

Uma das principais alegações no monitoramento e gerenciamento de redes de computadores, é que são inevitáveis a presença de lacunas de segurança em sistemas computacionais (BEJTLICH, 2013). Mesmo com o uso intensivo de ferramentas de restrição e contenção como, sistemas de prevenção e detecção de intrusos, *firewalls* e o uso de técnicas de melhores práticas para prevenção de incidentes de segurança, não são capazes de barrar as tentativas de intrusão que podem a qualquer momento transpor estas barreiras iniciais e se tornarem uma grande ameaça as organizações. Quando tratados de forma correta, os impactos com os incidentes podem ser minimizados.

Um incidente de segurança pode ser conceituado como qualquer evento adverso, comprovado ou sob suspeição, referente à segurança de sistemas da informação que pode provocar a perda de um dos princípios da tríade da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. (TIC-URFJ, 2017).

Situações que exemplificam alguns incidentes de segurança:

- Ataques de negação de serviços;
- Acesso ou uso não permitido de um sistema;
- Tentativas de obter acesso não autorizado a dados ou ao sistema;
- Alterações em um sistema, sem o conhecimento ou consentimento prévio do proprietário do sistema;
- Desrespeito às regras e a política de segurança vigente na organização.

2.5.1 - INCIDENTES DE SEGURANÇA EM CÂMERAS *IP*

A cada dia mais presentes em residências e organizações ao redor do mundo, o uso de circuitos de monitoramento e vigilância, compostos por câmeras *IP* é uma realidade, sobretudo pela evolução tecnológica promovida por tais dispositivos, que a cada dia tem se tornado mais eficientes em termos de qualidade, mais acessíveis em termos de custo e mais intuitivos, do ponto de vista de facilidade de instalação e configuração. Porém, como todo e qualquer dispositivo conectado a uma rede, as câmeras *IP* podem eventualmente, ser alvos de ataques. Atualmente existe um grande número de câmeras *IP* conectadas à *Internet,* em especial, em função do advento *IoT*, o que traz grande preocupação. Interfaces de gerenciamento desenvolvidas com a finalidade de facilitar a utilização e o acesso, bem como a redução de custos, fatalmente pecam no fator segurança. Dispositivos tradicionais e estabelecidos de computação, como computadores, *notebooks* e *smartphones*, em geral possuem ferramentas de segurança para mitigar eventuais ataques ou ainda, podem ter vulnerabilidades corrigidas via atualização de *software*. Dispositivos domésticos, inclusive *IoT,* tem sido alvo frequente de ataques, em especial os voltados a negação de serviço distribuído, ou simplesmente *DDoS*. Nem sempre uma atualização de *firmware* está disponível para corrigir eventuais vulnerabilidades de câmeras *IP*, por exemplo, tampouco existe suporte disponível. Em dispositivos como modems e roteadores domésticos por exemplo, existe um movimento recente de disponibilização de *custom firmwares*, desenvolvidos pela comunidade, mas trata-se de um processo lento que obviamente depende da popularidade do dispositivo em questão.

Tendo em vista o exposto, torna-se claro que os equipamentos legados continuam em pleno funcionamento e em grande parte dos casos, sem perspectiva de substituição. Nesse sentido, torna-se necessário o desenvolvimento de uma solução que possa ser incorporada à rede local, alterando a topologia inicial das soluções normalmente adotadas, por uma alternativa que mitigue os ataques normalmente praticados nesse cenário.

3 - METODOLOGIA

A plataforma escolhida para a implementação do presente projeto baseia-se no sistema operacional *FreeBSD 12.1 Release* e na imagem disponibilizada no site do projeto, em formato de cartão *SD*, voltada para a arquitetura *Raspberry Pi 3*. A plataforma Raspberry Pi, vem se tornado popular em soluções de hardware e software para aplicações embarcadas devido ao seu baixo custo. De acordo com Richardson e Wallace (2016) no livro *Getting Started with Raspberry Pi,* o *Raspberry* não se diferencia de um computador tradicional apenas pelo tamanho e preço, porém principalmente por sua capacidade de se integrar com os mais diversos projetos eletrônicos.

As aplicações de terceiros utilizadas para promover as funcionalidades esperadas são descritas a seguir:

- *ZoneMinder*;
- *MySQL Server 5.7*;
- *Nginx*;
- *fcgiwrap*;
- *PHP*.

Além disso, foi utilizado o serviço *hostapd*, presente no *base system* do sistema operacional *FreeBSD*, para prover a conectividade das câmeras *IP* via conexão de rede sem fio, incorporando ao dispositivo implementado a funcionalidade de ponto de acesso *WiFi*. A topologia completa utilizada no desenvolvimento da pesquisa é apresentada na Figura 3.1.

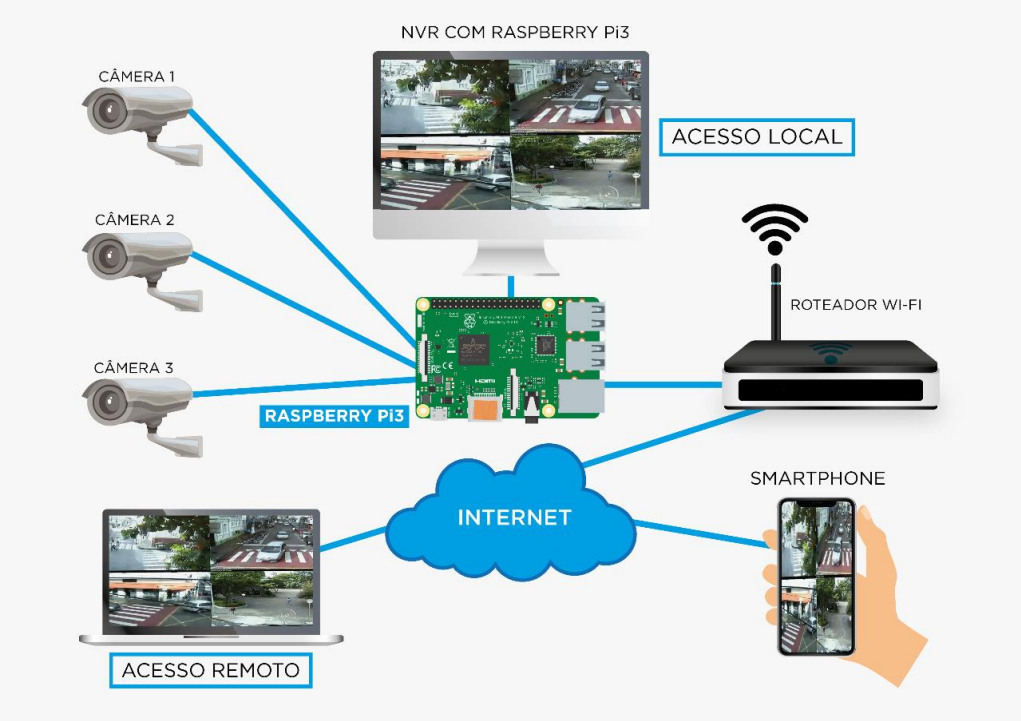

Figura 3.1 – Topologia utilizada para confecção do *NVR* portátil.
Fonte: Elaborado pelos autores (2019).

Para a instalação dos pacotes supracitados, foi utilizada a ferramenta *pkg*, utilitário que provê uma interface para manipulação de pacotes pré-compilados registrando, adicionando, removendo e atualizando pacotes no sistema. O comando utilizado é o informado a seguir:

 # pkg install zoneminder mysql57-server nginx fcgiwrap

O pacote referente à linguagem de programação *PHP* foi omitido do comando acima tendo em vista que o mesmo é instalado como dependência do pacote *zoneminder*. Tendo em vista a atualização frequente dos pacotes supracitados bem como da documentação referente ao processo, não se preocupe caso as versões dos *softwares* mencionados na presente seção sejam diferentes das efetivamente instaladas em seu sistema, de modo a não tornar o processo em questão obsoleto. Para que o processo de instalação transcorra sempre da melhor maneira possível,

recomendamos sempre a instalação do pacote principal e a posterior leitura das informações pós instalação que irão nortear todo o processo. Os comandos necessários para tanto são descritos a seguir:

 # pkg install zoneminder
 # pkg info -D zoneminder

Uma vez instalados os pacotes, iremos configurar cada um dos serviços envolvidos. O primeiro deles é o servidor de banco de dados *MySQL*, versão 5.7 ou superior. Os comandos abaixo irão automatizar a inicialização do serviço a partir do próximo *boot* e iniciar o serviço imediatamente, respectivamente:

 # sysrc mysq_server_enable="YES"
 # service mysql-server start

O próximo passo consiste na configuração do servidor *web nginx*. A aplicação de gerenciamento de câmeras será executada via interface *web*, utilizando o *nginx* como servidor. Os comandos abaixo irão automatizar a inicialização do serviço a partir do próximo *boot* e iniciar o serviço imediatamente, respectivamente:

 # sysrc nginx_enable="YES"
 # service nginx start

Ainda será necessário modificar o arquivo de configuração do *nginx*, denominado *nginx.conf*, localizado em */usr/local/etc/nginx*, para tanto, utilizaremos o editor de textos *easy editor*, ou simplesmente *ee*:

 # ee /usr/local/etc/nginx/nginx.conf

O arquivo em questão deve ter o seguinte conteúdo na seção *server*:

```
server {
        listen 80;

        root /usr/local/www/zoneminder;
        index index.php
        gzip off;

        location /cgi-bin/nph-zms {

                include fastcgi_params;
                fastcgi_param SCRIPT_FILENAME $request_filename;
                fastcgi_pass  unix:/var/run/fcgiwrap/fcgiwrap.sock;
        }

        location /zm/cache {

                alias /var/cache/zoneminder;
        }

        location /zm {

                alias   /usr/local/www/zoneminder;

                location ~ \.php$ {

                        if (!-f $request_filename) { return 404; }
                        include fastcgi_params;
                        fastcgi_param SCRIPT_FILENAME $request_filename;
                        fastcgi_index index.php;
                        fastcgi_pass unix:/var/run/php-fpm.sock;
                }
```

```
                location ~ \.(jpg|jpeg|gif|png|ico)$ {
                        access_log   off;
                        expires      33d;
                }

                location /zm/api/ {
                        alias   /usr/local/www/zoneminder;
                        rewrite ^/zm/api(.+)$ /zm/api/app/webroot/index.php?p=$1
last;
                }
        }
}
```

Para que o servidor *web nginx* possa executar *scripts CGI*, é necessário um *wrapper* externo, nesse caso, o *fcgiwrap*. Os comandos a seguir irão automatizar a inicialização do serviço a partir do próximo *boot,* definir o usuário de sistema responsável pela execução do serviço, definir o usuário do sistema “dono” do canal de comunicação entre o *wrapper* e servidor *web* e definir o número de câmeras que o servidor em questão gerencia, nesse caso quatro, respectivamente:

```
# sysrc fcgiwrap_enable="YES"
# sysrc fcgiwrap_user="www"
# sysrc fcgiwrap_socket_owner="www"
# sysrc fcgiwrap_flags="-c 4"
```

Conforme mencionado anteriormente, a linguagem *PHP* já é instalada como dependência do *zoneminder*. Ainda assim, algumas configurações são necessárias para que o suporte à linguagem esteja funcional. O primeiro deles diz respeito ao conteúdo do arquivo php-*fpm.conf*, localizado em */usr/local/etc* . O comando a ser

utilizado para a edição é o apresentado abaixo e o conteúdo a ser inserido é informado na sequência:

 # ee /usr/local/etc/php-fpm.conf

listen = /var/run/php-fpm.sock
listen.owner = www
listen.group = www
env[PATH] = /usr/local/bin:/usr/bin:/bin

Para automatizar a inicialização do serviço a partir do próximo boot e iniciar o serviço imediatamente, basta que os seguintes comandos sejam executados:

 # sysrc php_fpm_enable="YES"
 # service php-fpm start

Os últimos passos referem-se a configuração da base de dados do *zoneminder*. Desse modo, é necessário conectar-se ao servidor *mysql* instalado previamente como usuário *root*, em seguida criar o banco de dados denominado "*zm*", modificar os privilégios associados ao banco de modo a associá-lo ao usuário "*zmuser*" com a senha de acesso "*zmpass*" e por fim, popular a base de dados com o *dump* entitulado "*zm_create.sql*". Os comandos necessários para tanto são descritos a seguir:

 # mysql -u root -p

CREATE DATABASE zm;
GRANT ALL PRIVILEGES ON zm. TO 'zmuser'@'localhost' IDENTIFIED BY 'zmpass';*
FLUSH PRIVILEGES;
quit;

 # mysql -u root -p zm < /usr/local/share/zoneminder/db/zm_create.sql

Para automatizar a inicialização do serviço a partir do próximo boot e iniciar o serviço imediatamente, basta que os seguintes comandos sejam executados:

 # sysrc zoneminder_enable="YES"
 # service zoneminder start

4 - RESULTADOS

Após a instalação e configuração do sistema operacional e dos *softwares* envolvidos, basta acessar a interface de administração do *zoneminder* via qualquer navegador *web* para ter acesso à interface de administração. O endereço *IP* utilizado vai depender das configurações de rede especificadas na interface cabeada do *Raspberry Pi*, tendo em vista que a configuração referente ao *daemon hostapd* é voltada única e exclusivamente para a comunicação e gerenciamento das câmeras *IP* utilizadas.

A Figura 4.1 mostra o *dashboard* principal do *zoneminder* com algumas câmeras *IP* pré-configuradas.

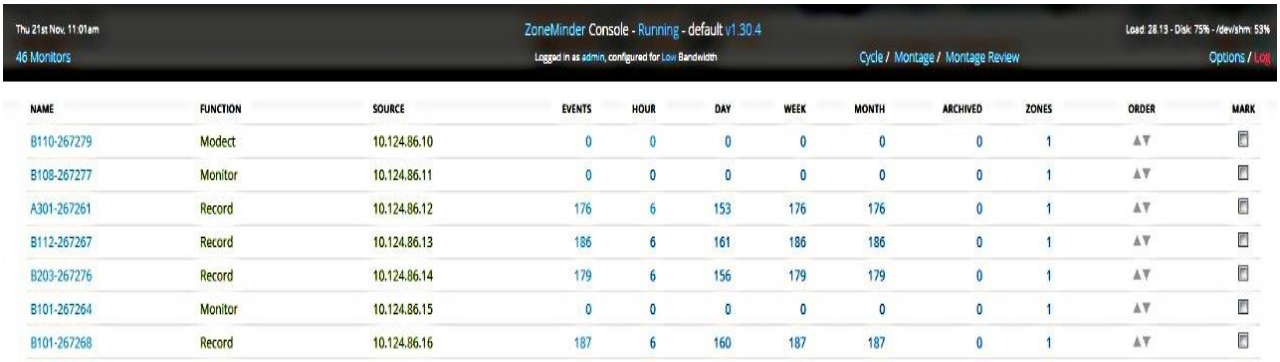

Figura 4.1 – *Dashboard* do *zoneminder.*
Fonte: Elaborado pelos autores (2019).

A configuração das câmeras *IP* é realizada individualmente e varia de acordo com a marca, modelo e recursos disponíveis. A Figura 4.2 apresenta as propriedades de configurações referentes à câmera *IP* utilizada em nossos testes, que contemplam: tipo de protocolo de captura utilizado, dados de autenticação baseados em usuário e senha, bem como endereço *IP* utilizado, resolução, paleta de cores e protocolo de comunicação. Já a figura 4.3 refere-se a configurações genéricas referentes à entrada do dispositivo exibida no *dashboard*, em especial nome com que o dispositivo será identificado, *codec* utilizado, modo de operação do dispositivo, quantidade de quadros por segundo e eventuais alarmes e gatilhos associados ao dispositivo, função utilizada para captura de foto ou vídeo no caso de detecção de movimentos, por exemplo.

Por fim, a Figura 4.4 apresenta uma captura de tela da câmera instalada em nosso ambiente de testes. Trata-se de um laboratório monitorado por vídeo em tempo real, utilizado como prova de conceito em nossos experimentos. A instalação de um maior número de câmeras depende única e exclusivamente da finalidade do projeto em questão.

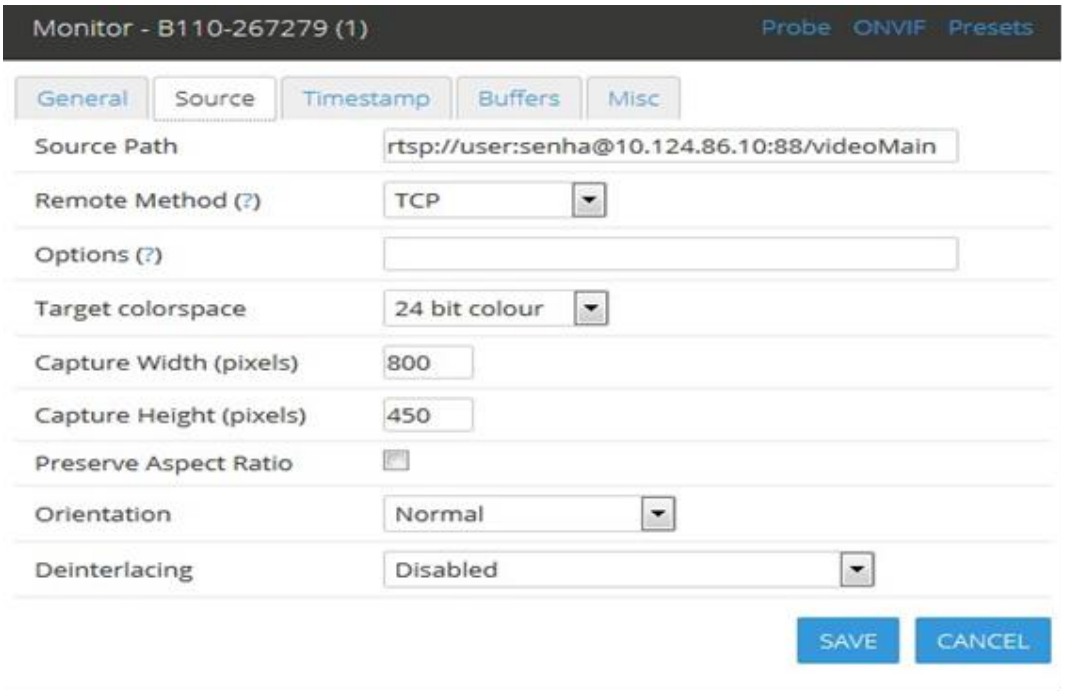

Figura 4.2 – Propriedades de configuração da câmera *IP.*

Fonte: Elaborado pelos autores (2019).

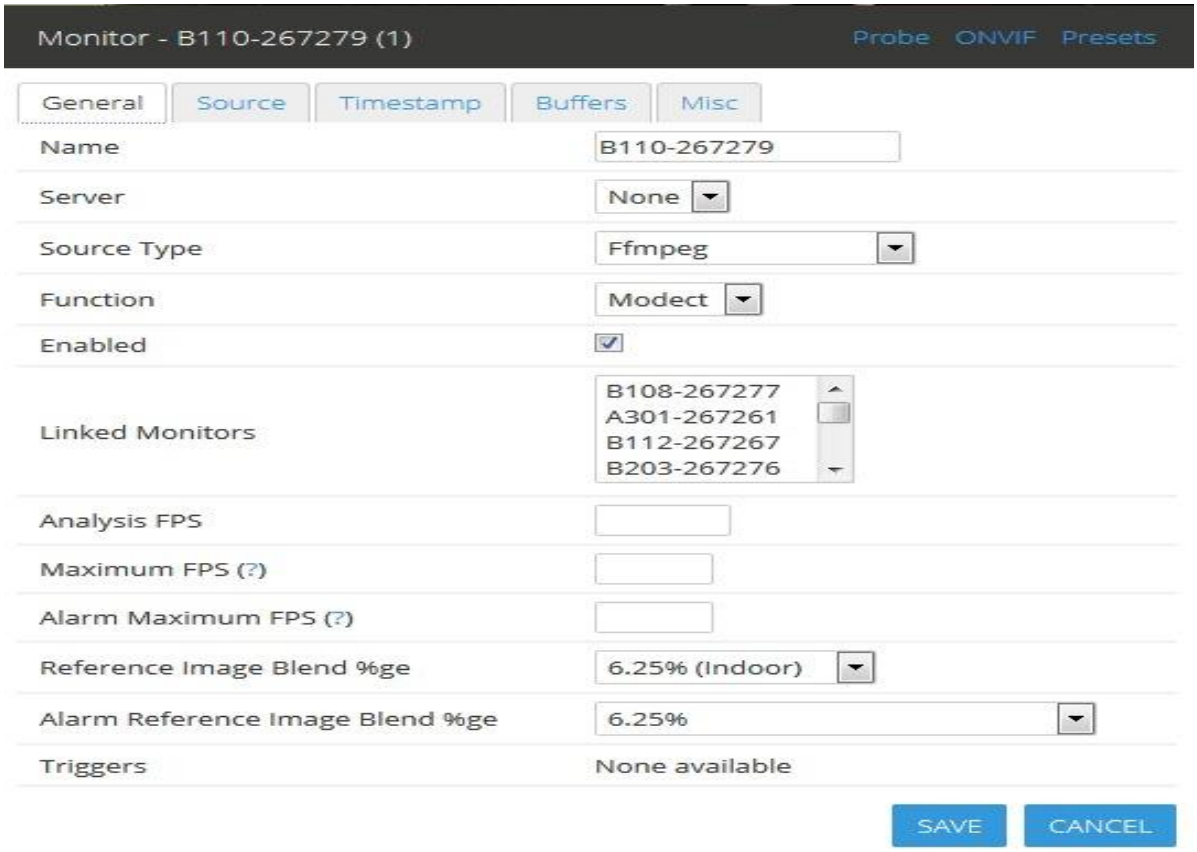

Figura 4.3 – Configurações gerais de uma câmera *IP* no *zoneminder.*

Fonte: Elaborado pelos autores (2019).

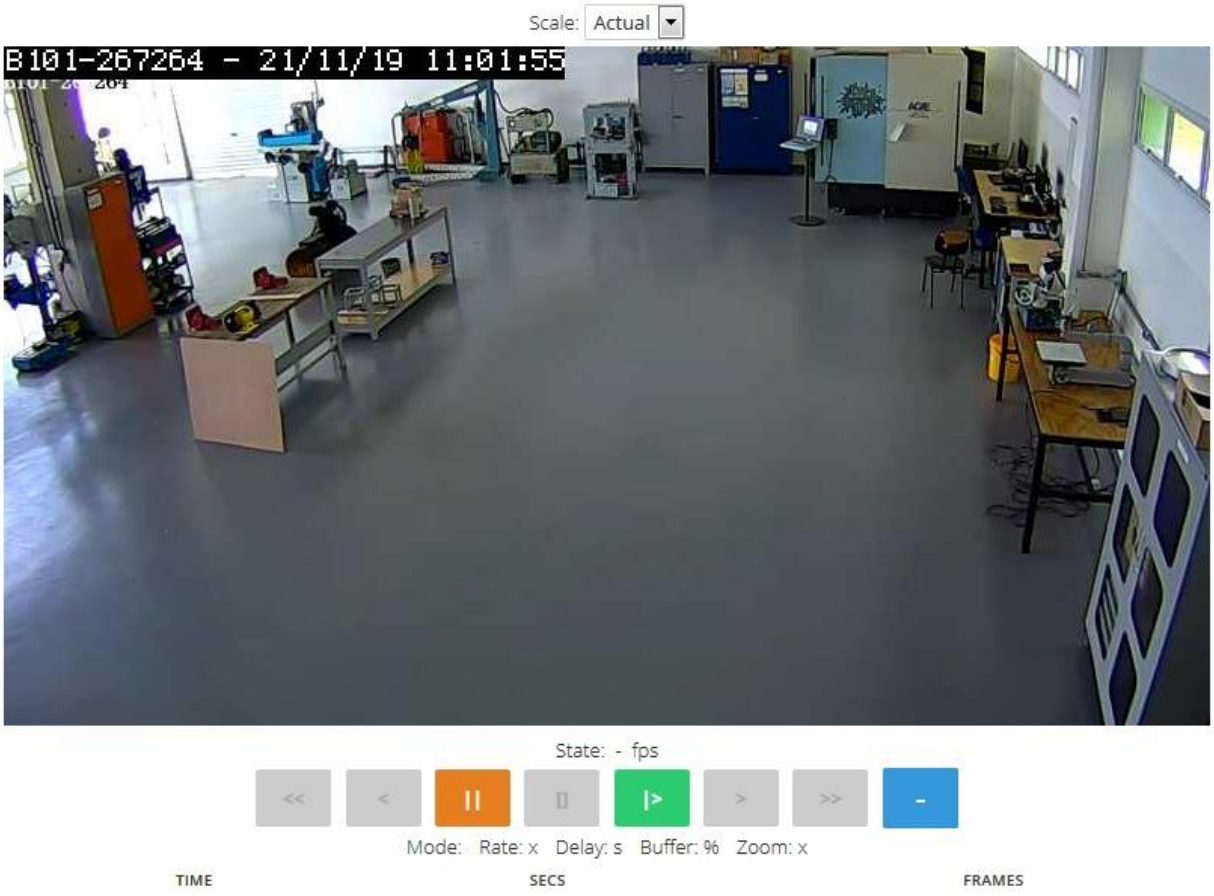

Figura 4.4 – Captura de tela da câmera instalada em nosso ambiente de testes.
Fonte: Elaborado pelos autores (2019).

A câmera utilizada em nossos testes é uma *FI9831W* da marca *FOSCAM*. Trata-se de uma câmera utilizada a título de empréstimo e, portanto, já previamente existente na instituição onde a pesquisa foi desenvolvida. A escolha da câmera justifica-se pelo fato de que, durante os testes iniciais de configuração, o equipamento se demonstrou compatível com a ferramenta utilizada, não requerendo dessa forma, a aquisição de um novo *hardware* específico para realização da prova de conceito. De acordo com pesquisas realizadas em fóruns de discussão e em documentações relacionadas ao *zoneminder* obtidas na *Internet*, a compatibilidade da ferramenta é bastante ampla, no entanto, cabe ressaltar que os desenvolvedores não garantem a compatibilidade do *software* com todo e qualquer dispositivo comercializado no mercado.

5 - DISCUSSÕES E CONCLUSÕES

A implementação de um dispositivo de rede portátil, de baixo custo, com inúmeras possibilidades de personalização, que pode ser facilmente inserido em ambientes domésticos ou corporativos, que permite centralizar a administração de câmeras *IP* existentes na rede local, podendo isolar o tráfego e eventuais vulnerabilidades frequentemente encontradas nesse tipo de equipamento do mundo exterior, representa uma contribuição significativa quando o assunto é segurança de redes e monitoramento baseado em imagens. Evidentemente, a utilização de dispositivos seguros, com possibilidades de atualização de *firmware* e longos períodos de suporte, são parte da solução tida como ideal, no entanto, equipamentos legados de baixo custo é a realidade de grande parte dos usuários desse tipo de equipamento, em especial, em países em fase de desenvolvimento como o Brasil, por exemplo. Sendo assim, tal solução torna-se indispensável para que o usuário exerça a função de observador e não de observado.

Uma questão importante que deve ser considerada é a quantidade de câmeras utilizadas. Dependendo da resolução da imagem gerada ou do algoritmo de compactação utilizado, é possível que o dispositivo portátil chegue a seu limite de processamento ou utilização de memória. Nesse sentido, bastaria a confecção de um *cluster* composto pelo número de nós necessários para administrar a quantidade de câmeras desejadas.

Outro fator que não foi mencionado no presente trabalho está relacionado aos dados gerados pelo sistema, uma vez que o mesmo disponibiliza também a função de monitoração e gerenciamento. Desse modo, imagens e vídeos são armazenados de acordo com gatilhos pré-configurados, como por exemplo, a detecção de movimentos. Nesse sentido, bastaria a inclusão de um dispositivo de armazenamento de rede, como um servidor *NFS*, por exemplo e o problema estaria resolvido, tendo em vista que se trata de um recurso de armazenamento remoto mapeado no dispositivo. Outra opção é a utilização de dispositivos externos, como um *hd* portátil, por exemplo. Ambas soluções são funcionais e devem ser escolhidas conforme a necessidade de portabilidade exigida pelo projeto.

Conforme mencionado anteriormente, a configuração das câmeras *IP* é realizada individualmente e varia de acordo com a marca, modelo e recursos disponíveis. Recomenda-se a leitura da documentação oficial e de fóruns de discussão relacionados ao tema para dúvidas mais pontuais relacionadas não só a configuração, mas também referentes a compatibilidade dos equipamentos.

Com a iminente adoção do protocolo *IPv6* como padrão, o número de câmeras *IP* diretamente conectadas à *Internet* deve aumentar exponencialmente. De mesmo modo, a chamada "*Internet* das Coisas", ou simplesmente *IoT*, deve conectar um número ainda maior de dispositivos inteligentes dos mais diversos tipos que vão desde eletrônicos (*smart TV's*, *media boxes* e afins), eletrodomésticos (geladeiras, torradeiras, cafeteiras) até dispositivos voltados à saúde e os já populares dispositivos vestíveis (*smartbands, smartwatches*). Sendo assim, os problemas relativos às câmeras *IP* apresentados no presente trabalho fatalmente passarão a atingir também os dispositivos supracitados e o dispositivo desenvolvido certamente poderão agregar novas funcionalidades de modo a contribuir também nesse sentido.

5.1 - TRABALHOS FUTUROS

Os passos envolvidos na criação e configuração do dispositivo apesar de não serem muito numerosos são minuciosos e podem induzir ao erro. Nesse sentido acreditamos que a criação de uma aplicação em formato de *script* capaz de automatizar os processos manuais necessários para a implementação seja de grande valia como trabalho futuro. A distribuição da aplicação em questão pode ser feita *online,* via repositórios de conteúdo *open source*, como o *GitHub*, por exemplo, ou ainda em em forma de aplicação oficial, disponibilizada diretamente por aplicações nativas do sistema operacional *FreeBSD*, como a suíte *pkg* ou via *ports.*

O aumento de funcionalidades do dispositivo desenvolvido é perfeitamente possível e viável, podendo este ser expandido e passando a agregar novos serviços e suportar novos tipos de dispositivos.

5.2 - AGRADECIMENTOS

À Sala IFSP-CIMNE, ambiente de pesquisa institucional viabilizado pelo acordo internacional firmado entre o *CIMNE – International Centre for Numerical Methods in Engineering* e o Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, que propiciou a infraestrutura necessária para o desenvolvimento da presente pesquisa.

REFERÊNCIAS BIBLIOGRÁFICAS

AHRENS, Benedikt. **GNewSense - O Ubuntu Livre.** 2009. Disponível em: <https://www.hardware.com.br/artigos/gnewsense/>. Acesso em: 17 nov. 2019.

ASHTON, K. **That 'Internet of Things' Thing in the Real World, Things Matter More Than Ideas.** Disponível em: <http://www.rfidjournal.com/articles/view?4986>. Acesso em: 27 jul. 2019.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. **The Internet of Things: A Survey Computer Networks**, v. 54, n. 15, p. 2787-2805, 2010.

BEJTLICH, R. **The Practice of Network Security Monitoring: understanding incident detection and response.** São Francisco, CA, USA: No Starch Press, 2013.

BOLDT, Martin, **Privacy-Invasive Software, Blekinge Institute of Technology**, 2010 p. 11.

CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. 2017.

DATASUS – Departamento de Informática do SUS. **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Ministério Saúde.** Disponível em: <http://datasus.saude.gov.br/images/MS%20-%20Metodologia%20de%20Gesto%20de%20Riscos_v20141105.pdf>. Acesso em: 12 nov. 2019.

ERBSCHLEO, Michael. **Trojans, Worms and Spyware – A Computer Security Professional's Guide to Malicious Code**, Elsevier Butterworth–Heinemann, 2005, p.19.

FILIOL, Eric. **Computer Viruses: from Theory to Application**, Springer, 2005, p. 83.

IBSG-CISCO.**The Internet of Things**. 2011. Disponível em: <http://share.cisco.com/internet-ofthings.html>. Acesso em: 10 ago. 2019.

INCAPSULA. **Malware Types.** Disponível em: <https://www.incapsula.com/webapplication-security/malware-detection-and-removal.html>. Acesso em: 25 out. 2019.

International Conference on Digital Government Research. ACM, 2012. p. 302-303. VALÉRY, N. **Welcome to the Thingternet: Things, Rather than People, are About to Become the Biggest Users of the Internet**. The Economist, v. 21, 2012.

ITU-International Telecommunication Union. **ITU Internet Reports 2005: The Internet of Things.** Geneva, 2005. Disponível em: <http://www.itu.int/osg/spu/publications/internetofthings/>. Acesso em: 20 mai. 2018.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva**. 3. Ed. Rio de Janeiro: Elsevier, 2003. 160p.

SIMÕES, José Carlos Ferrer. **ANÁLISE DA MATURIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DOS ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA FEDERAL DIRETA.** Centro Universitário de Brasília (UniCEUB/ICPD). Monografia de Pós-graduação Lato Sensu em Governança em Tecnologia da Informação. 2014.

PAUL BÄCHER et al. (2006) **"The Nepenthes Platform: An Efficient Approach to Collect Malware"** In Diego Zamboni and Christopher Krügel, editora RAID: volume 4219 do LNCS, p. 165–184, Springer.

PANDA SECURITY. **Worms** Disponível em: <https://www.pandasecurity.com/pt/security-info/classic-malware/worm/>. Acesso em: 16 out. 2019.

PURI, Ramneek. **Bots & Botnet: An Overview.** SANS Institute, v. 3, p. 10, 2003.

RICHARDSON, M.; WALLACE, S. **Getting Started With Raspberry Pi**. Maker Media, 2016.Disponível em: <https://media.digikey.com/pdf/Data%20Sheets/O'Reilly_PDFs/Getting_Started_With_Raspberry_Pi_3E_9781680452464.pdf>. Acesso em: 15 nov. 2019.

SAAVEDRA, Y. M., BARQUET, A. P., ROZENFELD, H., FORCELLINI, F. A., &OMETTO, A. R. (2013). **Remanufacturing in Brazil: Case Studies on the Automotive Sector**. Journal of Cleaner Production, 53, 267-276.

URFJ /TIC – Universidade Federal do Rio de Janeiro/Superintendência de Tecnologia da Informação e Comunicação. **Incidentes de Segurança da Informação.** Disponível em: <https://tic.ufrj.br/index.php/o-que-sao-incidentes>. Acesso em: 21 out. 2019.

WEISER, M. **The Computer for the 21st Century**. Scientific American, v. 265, p. 94–104, 1991.