

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Augusto Moura Alves Silva

Segurança para câmeras IP

Uberlândia, Brasil

2018

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Augusto Moura Alves Silva

Segurança para câmeras IP

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito exigido parcial à obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Luiz Cláudio Theodoro

Coorientador: David Arantes Pereira

Universidade Federal de Uberlândia – UFU

Faculdade de Ciência da Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2018

Resumo

As câmeras IP estão cada vez mais presentes nas residências e comércios do mundo inteiro, isso ocorre devido às vantagens que o dispositivo fornece como seu baixo custo em infraestrutura, facilidade na instalação e configuração e no monitoramento remoto das imagens capturadas em tempo real e com alta resolução. Contudo, a segurança nesse cenário tecnológico passa a ser um desafio, devido a inúmeras vulnerabilidades e ameaças que vem crescendo cada vez mais. Sendo assim, esse trabalho visa solucionar esses problemas, tendo por objetivo o estudo teórico e prático para descrever as melhores práticas a fim de garantir a segurança de um sistema de vigilância que utiliza câmeras IP. A sua instalação é simples e prática, o que possibilita que usuários comuns instalem o dispositivo sem a necessidade de uma mão-de-obra especializada, mas é de fundamental importância o cumprimento de uma política de segurança adequada.

Palavras-chave: câmera IP, segurança, vulnerabilidades, rede, DDoS.

Lista de ilustrações

Figura 1 – Camada de aplicação	13
Figura 2 – Protocolos e redes no modelo TCP/IP	13
Figura 3 – A camada de rede	14
Figura 4 – Pilha de protocolo de Internet e modelo de referência OSI	16
Figura 5 – Camadas do protocolo TCP/IP	16
Figura 6 – Exemplo do modo de infra-estrutura de redes sem fio	18
Figura 7 – Rede sem fio no modo Ad-Hoc	19
Figura 8 – Classificação pela abrangência das redes sem fio.	20
Figura 9 – Princípios fundamentais da segurança da informação.	21
Figura 10 – Processo de criptografia simétrica.	28
Figura 11 – Processo de autenticação com servidor.	30
Figura 12 – Câmera IP externa fixa com infravermelho	33
Figura 13 – Câmera IP dome fixa	34
Figura 14 – Câmera IP PTZ	34
Figura 15 – Câmera IP PTZ	35
Figura 16 – Fluxo de infecção de ELF PERSIRAL.A	40
Figura 17 – Vulnerabilidades por ano	42
Figura 18 – Nível de segurança.	49
Figura 19 – Diagrama representativo do sistema desenvolvido	49
Figura 20 – Roteador utilizado para conectar as câmeras, a central e o computador pessoal do usuário.	50
Figura 21 – Câmera utilizada para realizar a aquisição das imagens de vigilância.	51
Figura 22 – Computador e memória não volátil utilizados.	51
Figura 23 – Figura protocolos de comunicação – Camadas do modelo TCP/IP e seus respectivos protocolos utilizados.	52
Figura 24 – Imagem capturada em um ambiente com luz.	53
Figura 25 – Imagem capturada em um ambiente sem luz.	54
Figura 26 – Hikvision Password Reset.	54
Figura 27 – Bloqueio de conta após falhas de login.	55
Figura 28 – scanner com NMAP utilizando o script rtsp-url-brute para encontrar as URL's do RTSP.	56
Figura 29 – Ativando o bloqueio de registro irregular.	56

Lista de abreviaturas e siglas

AIC	Availability, Integrity and Confidentiality
CFTV	Circuito Fechado de Televisão
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FPS	Frames per second
FTP	File Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IDEA	International Data Encryption Algorithm
ISO	International Standards Organization
IoT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network
HTTP	Hyper Text Transfer Protocol
MSK	Master Session Key
OSI	Open Systems Interconnection
PoE	Power Over Ethernet
POP3	Post Office Protocol version 3
RC	Ron's Code ou Rivest Cipher
RTP	Real-time Transport Protocol
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol

TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
WLL	Wireless Local Loop
WPA	Wi-fi Protected Access
WPAN	Wireless Personal Area Network

Sumário

1	INTRODUÇÃO	9
1.1	Objetivos	11
1.1.1	Objetivo geral	11
1.1.2	Objetivos específicos	11
1.2	Organização da monografia	11
2	REDES DE COMPUTADORES	12
2.1	A Internet	12
2.2	Arquitetura de camadas	12
2.2.1	Camada de protocolos	12
2.2.2	Camada de aplicação	12
2.2.3	Camada de transporte	13
2.2.4	Camada de rede	14
2.2.5	Camada de enlace	15
2.2.6	Camada física	15
2.3	Modelo de referência OSI	15
2.4	Modelo de referência TCP/IP	16
2.5	Redes sem fio	17
2.6	Padrões de comunicação	19
3	SEGURANÇA DA INFORMAÇÃO	21
3.1	Princípios fundamentais de segurança	21
3.1.1	Disponibilidade	22
3.1.2	Integridade	22
3.1.3	Confidencialidade	22
3.1.4	Autenticidade	23
3.1.5	Não-repúdio	23
3.1.6	Conformidade	23
3.2	Definições de segurança	23
3.2.1	Vulnerabilidades	23
3.2.1.1	Vulnerabilidade Naturais	23
3.2.1.2	Vulnerabilidade Física	24
3.2.1.3	Vulnerabilidades de Hardware	24
3.2.1.4	Vulnerabilidade de Software	24
3.2.1.5	Vulnerabilidade de Armazenamento	24
3.2.1.6	Vulnerabilidade de Comunicação	24

3.2.1.7	Vulnerabilidade Humana	24
3.2.1.8	Vulnerabilidade Organizacional	25
3.3	Ameaça	25
3.3.1	Malware	25
3.3.1.1	Vírus	26
3.3.1.2	Worm	26
3.3.1.3	Bot e Bootnets	26
3.3.1.4	Spyware	26
3.3.1.5	Backdoor	27
3.3.1.6	Trojan	27
3.4	Mecanismos de segurança	27
3.4.1	Segurança em LANs sem fio	27
3.4.1.1	Criptografia de dados	27
3.4.1.2	Wired Equivalent Privacy (WEP)	29
3.4.1.3	Wi-fi Protected Access (WPA)	29
3.4.1.4	Wi-fi Protected Access - Personal	30
3.4.1.5	Wi-fi Protected Access - Enterprise	30
3.4.1.6	Protocolo de Autenticação Extensível - EAP	31
3.4.2	Honeypot	31
3.4.3	FIREWALL	31
4	CÂMERAS IP	32
4.1	Introdução a câmeras IP	32
4.1.1	Primeira câmera IP	32
4.1.2	Tipos de câmeras IP	32
4.1.3	Componentes internos de uma câmera IP	34
4.1.4	Vantagens das câmeras IP	35
4.1.5	Diretrizes para um projeto de vigilância IP	37
4.2	Ameaças e vulnerabilidade em câmeras IP	39
4.2.1	Ataques	43
4.3	Melhores práticas de segurança em câmeras IP	45
4.3.0.1	Recomendações para os usuários	46
4.3.0.2	Recomendações para os fabricantes	47
5	DESENVOLVIMENTO PRÁTICO	49
5.1	Dispositivos	49
5.2	Protocolos de comunicação	51
5.3	Software	52
5.4	Considerações sobre o desenvolvimento	53
5.5	Avaliação do fabricante	56

6	CONCLUSÃO	58
	REFERÊNCIAS	59

1 Introdução

O termo segurança, refere-se à uma das mais importantes e antigas demandas humanas, que durante séculos, fizeram com que o homem investisse tempo e recursos em soluções que pudessem proteger e prevenir seus bens patrimoniais e sua integridade física de ataques e ameaças.

A evolução tecnológica colaborou para o surgimento de novas formas de ataques e ameaças, e em paralelo, a evolução dos mecanismos de segurança se tornou uma necessidade fundamental. Várias foram as criações que ajudaram as pessoas e organizações a se protegerem nestas situações, entre elas, as câmeras de monitoramento, como um dos recursos de segurança mais conhecidos, que podem ser usadas para captar e gravar as imagens de um determinado local, trazendo assim, possibilidades de monitoramento.

Para se construir um sistema de monitoramento, existem diferentes tecnologias disponíveis e eficientes. O circuito fechado de televisão (CFTV), que consiste num conjunto de câmeras que captam as imagens e as transmitem até um sistema de televisão, são bastante populares e acessíveis à população.

Os sistemas atuais podem transmitir as imagens das câmeras através de cabos de rede *Ethernet* ou através de rede WiFi por meio de dispositivos *Wireless*, podendo gravar as imagens capturadas pelas câmeras em um computador local ou até mesmo na nuvem, proporcionando um maior conforto, comodidade e flexibilidade. Uma rede sem fio transmite dados utilizando sinais de rádio frequência e infravermelho que permitem mobilidade contínua através de sua área de abrangência(BEZERRA, 2014).

As câmeras IP (Internet Protocol), conhecidas também por câmeras de rede, proporcionam uma maior qualidade de imagem, facilidade na instalação, além de poder acessar e controlar as gravações através de um navegador web, conectado em uma rede IP, como a LAN, Internet ou intranet.

Para um CFTV é necessário, no entanto, uma atenção em especial, pois pode se tornar um alvo fácil de *hackers* já que possuem vulnerabilidades que possibilitam ataques ou invasões. Isto é gerado pelo fato de que as câmeras CFTV não são apenas câmeras, mas computadores com sistemas operacionais que executam *softwares* e estão efetivamente conectadas na Internet.

As empresas tendem a fabricar produtos da forma mais simplificada possível para facilitar a sua instalação e utilização, para que isso tenha efeito, é necessário que o fabricante deixe desativados alguns dos seus recursos de segurança, o que torna o produto mais vulnerável ainda, pois as informações de fábrica podem ser facilmente acessadas através

dos manuais disponibilizados no site dos fabricantes, além de que a grande maioria dos usuários utilizam os equipamentos com configuração de fábrica (*Default*), possibilitando o acesso não autorizado de muitos indivíduos à esses equipamentos (RUFINO, 2005).

Segundo Cluley Graham, as câmeras CFTV são vulneráveis por estarem configuradas com credenciais fracas ou com login padrão, e aceitam conexões de qualquer outra pessoa conectada à Internet, o que facilita o ataque contra estes dispositivos por meio da força bruta (CLULEY, 2015).

Outra forma possível e comum de ataque é por *malwares*, códigos maliciosos programados para realizar atividades maliciosas e danosas em um computador (CERT, 2012). Uma vez infectados, os dispositivos podem ser comandados em massa para executar ataques de negação de serviço, também conhecido como Distributed Denial of Service (DDoS).

De fato, a popularização da Internet das Coisas (IoT) possibilitou um aumento significativo de sistemas potencialmente vulneráveis a infecção, e como consequência disso, originou os *botnets*, que são redes de centenas ou milhares de máquinas comprometidas (bots), também chamadas de Zumbis, que são controladas remotamente por uma unidade de controle chamada *botmaster* (BÄCHER P.; WICHERSKI, 2007).

Uma *botnet* pode ser composta por diversas coleções de dispositivos, como laptops, servidores, telefones, impressoras, roteadores, câmeras ou qualquer outro dispositivo que esteja conectado à Internet e que possa executar programas (DUCKLIN, 2016).

Em meio a todo o processo de evolução de equipamentos e sistemas envolvendo segurança, pudemos acompanhar várias ameaças aos sistemas relacionados até aqui. Uma das maiores ameaças aconteceu em 2016, considerando ataques por hacker denominada Mirai. Consiste em um código malicioso utilizado para realizar um DDoS, inicialmente executado contra a Dyn, uma empresa de infraestrutura de Internet que oferece serviços de DNS para alguns dos principais sites no mundo como o Amazon, Netflix, Spotify, Twitter, Tumblr, SoundCloud e outros. O *malware* Mirai é capaz de assumir dispositivos conectados a Internet, como câmeras de vídeo CFTV, roteadores, gravadores de vídeo digital e outros (KREBS, 2016b).

Com o intuito de aprofundar os conhecimentos sobre ataques, em especial, em ambientes com monitoramento via câmera IP, discutir as fragilidades e propor práticas ou soluções de segurança, este trabalho pode gerar resultados interessantes e práticas que ajudem usuários em geral a proteger melhor seus ativos digitais.

1.1 Objetivos

1.1.1 Objetivo geral

O objetivo desse trabalho é realizar um estudo para articular e confrontar as informações adquiridas através dos conhecimentos teóricos da literatura pesquisadas em livros, artigos científicos e sites da Internet, possibilitando abranger os principais conceitos de segurança da informação, conceitos de redes de computadores, além de buscar as vulnerabilidades existentes e expor recomendações para os fabricantes afim de minimizar os problemas encontrados.

1.1.2 Objetivos específicos

O presente estudo tem como objetivos específicos:

1. Descrever os conceitos de redes de computadores;
2. Abordar os requisitos de segurança da informação;
3. Apresentar o funcionamento e os fornecedores das câmeras IP;
4. Relacionar possíveis ataques;
5. Identificar as vulnerabilidades;
6. Propor recomendações e orientações sobre como sanar as falhas de segurança.

1.2 Organização da monografia

O próximo capítulo deste trabalho aborda os princípios fundamentais e alguns conceitos sobre Redes de Computadores. No capítulo 3 será apresentada os conceitos de segurança da informação, no capítulo seguinte será apresentado uma visão geral acerca da tecnologia envolvendo Câmera IP, como por exemplo, tipos de câmeras IP, suas vantagens, vulnerabilidades, melhores práticas de segurança e recomendações. Já no capítulo 5, será desenvolvido um ambiente prático executando as melhores práticas que podem ser adotadas como forma de proteção contra essas ameaças e vulnerabilidades, a fim de realizar as considerações finais sobre o estudo realizado.

2 Redes de computadores

2.1 A Internet

A Internet consiste em uma rede que interconecta milhares de dispositivos computacionais ao redor do mundo, esses dispositivos também são chamados de sistemas finais, e cada vez mais, novos dispositivos estão sendo desenvolvidos e adaptados para se conectarem com a Internet, tais como: TVs, consoles para jogos, webcams, câmeras, automóveis, smartphones e outros. (KUROSE, 2010)

Para que esses dispositivos possam se conectar a uma rede e se comunicarem, são necessários inúmeros componentes e camadas na rede como enlaces de comunicação, comutadores de pacotes, protocolos, entre outros, que possuem papéis específicos que juntos possibilitam a existência da Internet.

2.2 Arquitetura de camadas

2.2.1 Camada de protocolos

A comunicação entre os sistemas que compõem uma rede só é possível devido à um conjunto de regras que são chamadas de protocolos de comunicação. Em cada camada existe um conjunto de protocolos, onde cada um possui uma função.

Segundo Kurose, uma camada de protocolo pode ser implementada em *hardware*, *software* ou numa combinação de *software* e *hardware*. Geralmente na camada de aplicação são implementados protocolos no *software* como os protocolos HTTP (*Hypertext Transfer Protocol*) e SMTP (*Simple Mail Transfer Protocol*), na camada física e na camada de enlace, normalmente o protocolo é implementado no *hardware*, ou seja, em uma placa de interface de rede, por exemplo placa de rede *Ethernet* ou *Wi-Fi*. Já a camada de rede quase sempre possui uma implementação no *hardware* e no *software*.

O conjunto de protocolos das camadas da rede são denominados pilha de protocolos, que são divididas em cinco partes: camada física, de enlace, de rede, de transporte e de aplicação (KUROSE, 2010).

2.2.2 Camada de aplicação

A camada de aplicação engloba vários protocolos que realizam a comunicação entre as aplicações, como por exemplo o FTP (*File Transfer Protocol*), HTTP (*HyperText Transfer Protocol*), TELNET, SMTP (*Simple Mail Transfer Protocol*), DNS (*Domain*

Name System), POP3 (*Post Office Protocol version 3*) e RTP (*Real-time Transport Protocol*).

A comunicação da camada de aplicação com a camada de transporte se dá através de uma porta, essas portas indentificam o protocolo de comunicação. Existe a diferença entre os protocolos da camada de aplicação com as aplicações, os protocolos têm a função de definir como os processos irão se comunicar e como irão tratar as mensagens, para expor o que foi solicitado pelo usuário, já as aplicações são as interfaces que os usuários interagem .

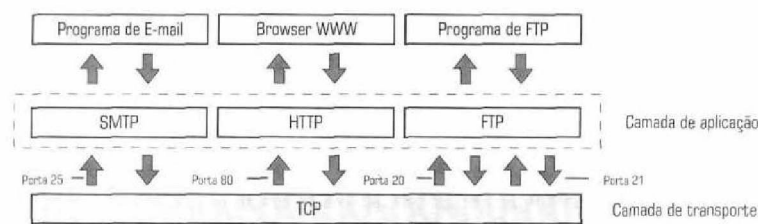


Figura 1 – Camada de aplicação

Fonte: (Gabriel Torres, Redes de computadores curso completo)

2.2.3 Camada de transporte

A camada de transporte fica entre a camada de aplicação e as camadas de nível físico, é responsável por transferir os dados entre dois sistemas finais, independente da aplicação, tipo ou configuração das máquinas e redes físicas usadas. Fornece serviços de comunicação lógica para a camada de aplicação, ela transforma as mensagens da camada de aplicação em fragmentos adicionados de cabeçalhos, também chamados de segmentos, e repassa para a camada de rede do sistema final. Seus protocolos são implementados nos sistemas finais e os principais são o TCP (*Transmission Control Protocol*) e o UDP (*User Datagram Protocol*) conforme ilustrado na figura 2. (KUROSE, 2010).

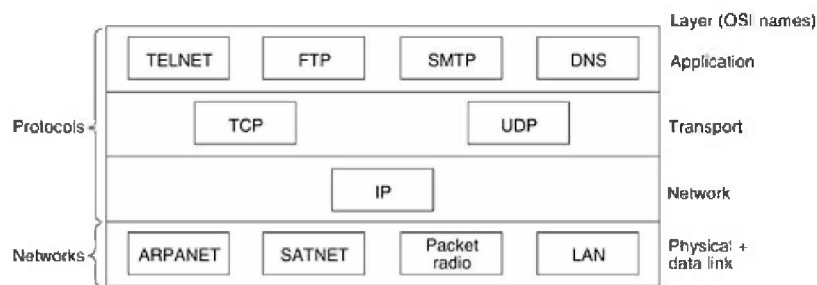


Figura 2 – Protocolos e redes no modelo TCP/IP

Fonte: (Tanenbaum, 4ª edition, Computer Networks)

2.2.4 Camada de rede

A camada de rede tem o papel de transportar os pacotes de um hospedeiro reme-
tente para um hospedeiro destinatário, esse transporte consiste em duas funções princi-
pais: repasse e roteamento. O repasse refere-se à ação local realizada pelo roteador para
transportar um pacote do enlace de entrada até um enlace de saída apropriado, já o ro-
teamento é quando a camada de rede determina a rota ou o caminho que os pacotes têm
que percorrer desde a fonte até o destino, como podemos ver na figura 3.

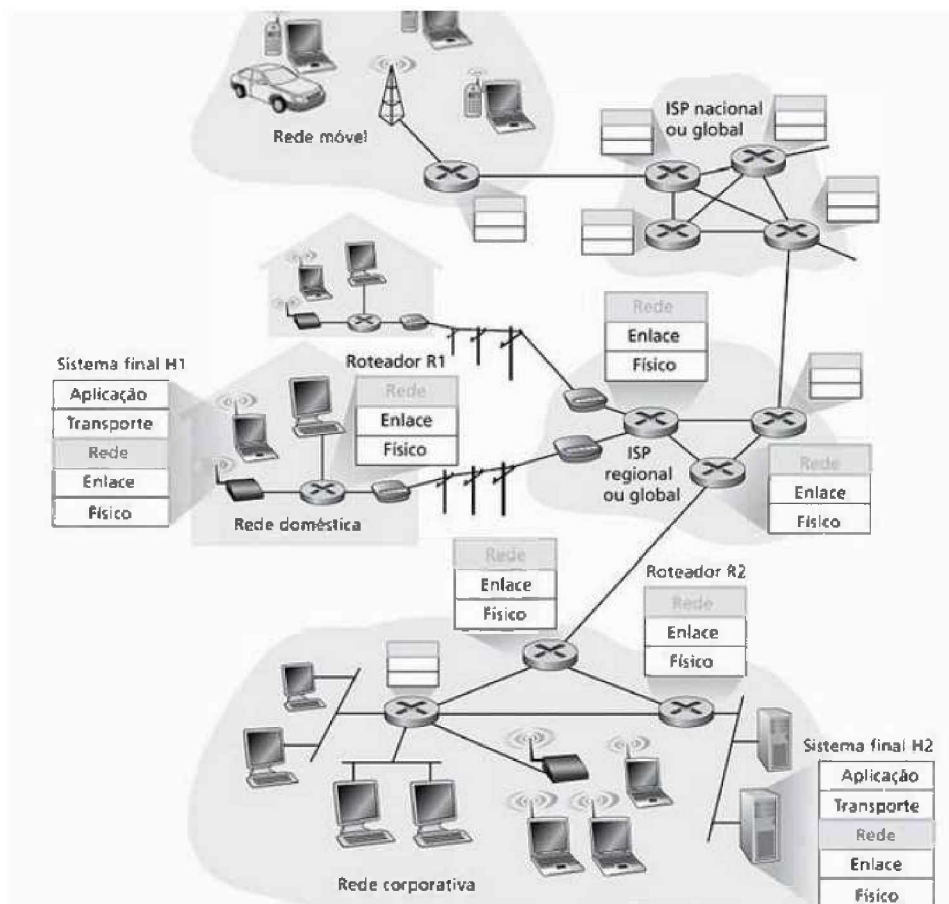


Figura 3 – A camada de rede

Fonte: (Kurose, 2010 p.230)

Cada roteador tem uma tabela de repasse, onde ele examina um campo do cabeçalho do pacote que está chegando e indexa o valor na sua tabela de repasse, o resultado dessa tabela indica para qual das interfaces de enlace o pacote deve ser repassado (KUROSE, 2010).

A camada de rede também é responsável por controlar o congestionamento de pacotes, que acontece quando há uma fila de pacotes no mesmo caminho da rede, gerando instabilidade e atraso de trânsito dos pacotes.

Existem diversos outros problemas que podem surgir no transporte de um pacote

de uma rede para outra, como por exemplo: o tamanho excessivo dos pacotes, protocolos diferentes, endereçamento diferente utilizados pelas redes. Cabe à camada de rede superar todos esses problemas para permitir que redes heterogêneas sejam interconectadas (TANENBAUM, 2011).

O ARP, ICMP, IP(IPv4, IPv6), X.25 e o Host/IMP são exemplos de protocolos da camada de rede.

2.2.5 Camada de enlace

A camada de enlace é responsável pelo endereçamento e controle de envio e recepção de quadros, ela faz com que o transmissor divida os dados de entrada em quadros de dados e os transmite sequencialmente da camada de rede de um dispositivo para a camada de rede de outro, podendo ser controlado tanto em *software* quanto em *firmware* ou *chipsets*.(TANENBAUM, 2011).

2.2.6 Camada física

A camada física é também chamada de camada de abstração de *hardware*, tem a função de transmitir os datagramas pelo meio físico buscando um caminho mais curto e confiável. Essa camada é responsável pelo endereçamento e tradução de nomes e endereços lógicos em endereços físicos, gerenciamento do tráfego e das taxas de velocidades nos canais de comunicação, estabelece e encerra conexões, notifica e corrige falhas, além de tratar os meios de comunicação à nível de *hardware*, tratando os sinais eletrônicos, conectores, dimensões físicas, níveis de tensão, características mecânicas e elétricas (TANENBAUM, 2011).

É uma das camadas mais importantes, pois possibilita o transporte dos pacotes de maneira mais eficiente com algoritmos de roteamento, comutação de pacotes, encapsulamento e estabelecimento da chamada.

2.3 Modelo de referência OSI

O modelo de referência OSI (*Open Systems Interconnection*), foi desenvolvido pela ISO (*International Standards Organization*) com o objetivo de padronizar os protocolos empregados nas diversas camadas, o modelo trata da interconexão de sistemas que estão abertos à comunicação com outros sistemas e ele possui sete camadas: física, de enlace, de rede, de transporte, de sessão, de apresentação e de aplicação.

No processo de transmissão de um dado, cada camada pega o dado da camada superior, acrescenta informações pelas quais ela seja responsável e passa os dados para a camada inferior, num processo chamado encapsulamento.(TANENBAUM, 2011)



Figura 4 – Pilha de protocolo de Internet e modelo de referência OSI

Fonte: (Kurose, 2010 p.38)

2.4 Modelo de referência TCP/IP

O TCP/IP (Protocolo de Controle de transmissão de Internet) é um conjunto de protocolos de comunicação, nos quais os principais são TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão) e o IP (*Internet Protocol* – Protocolo de Interconexão). O TCP/IP possui 4 camadas: Aplicação, Transporte, Internet, Interface com a rede, ilustradas na figura 4.

Atualmente o TCP/IP é o protocolo mais usado em redes locais. Isso se deve basicamente a popularização da Internet, a rede mundial de computadores, já que esse protocolo foi criado para ser usado na Internet. (TANENBAUM, 2011)

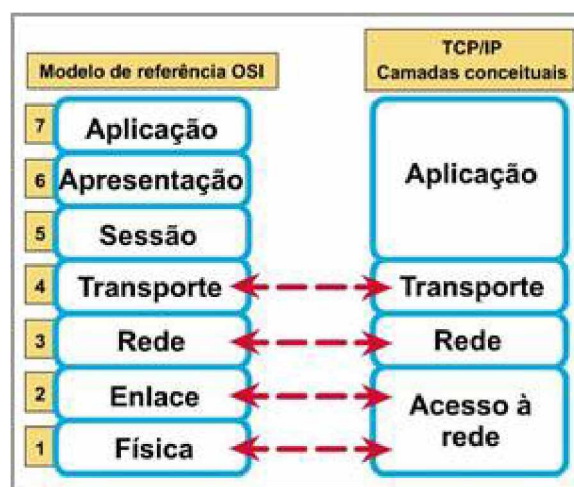


Figura 5 – Camadas do protocolo TCP/IP

Fonte: Cisco NETWORKING ACADEMY PROGRAM, 10 jun 2007

Devido ao seu tamanho e topologia, as redes TCP/IP podem ser classificadas de várias formas, entretanto as mais comuns são: Local Area Network (LAN) e Wide Area Network (WAN).

- Local Area Network (LAN) são redes com uma extensão geográfica restrita e privada em local físico como em uma empresa ou em uma casa, ela é limitada por uma faixa de IP restrita, com uma máscara de rede.

- Wide Area Network (WAN) as redes WAN possuem uma abrangência geográfica maior do que nas redes LAN, como o campus de uma universidade, uma cidade ou um país. A principal característica dela é a escalabilidade, ela permite que grandes empresas com milhares de computadores trafeguem uma grande quantidade de informação entre filiais.

2.5 Redes sem fio

Uma rede sem fio, consiste em uma rede conectada por equipamentos que usam rádio frequência (comunicação via ondas de rádio) ou comunicação via infravermelho, ou seja, não há necessidade de utilizar cabos.

As vantagens para o uso de uma rede sem fio consistem na facilidade de instalação já que não é necessário a instalação de cabos pelas paredes e pisos, na flexibilidade pois a rede sem fio permite atingir ambientes internos e externos onde não seria possível chegar por redes cabeadas, e na mobilidade já que permite aos usuários o acesso à informação em tempo real e em qualquer lugar.

As principais desvantagens das redes sem fio consistem no quesito segurança, propagação de sinal e restrições. Gabriel Torres (2001) cita algumas características que influenciam nas restrições:

- Imposição de órgãos regulamentadores limitando a largura de banda;
- Interferência na propagação do sinal pelo meio, já que o meio é domínio público;
- Alto consumo de energia dos dispositivos móveis.

De acordo com Rufino, existem dois tipos de funcionamento para as redes sem fio: Infraestrutura e Ad-Hoc.

Para redes sem fio funcionando no modo infraestrutura, é necessário um equipamento central que possibilita uma administração e concentração em um só ponto de todos os dispositivos clientes, possibilitando o controle de todos os dispositivos conectados com políticas de segurança como autenticação, autorização, filtro de pacote, controle de banda

e criptografia, além de possibilitar a interligação com a Internet Wi-Fi ou com redes cabeadas, conforme observado na figura 5.(RUFINO, 2005)

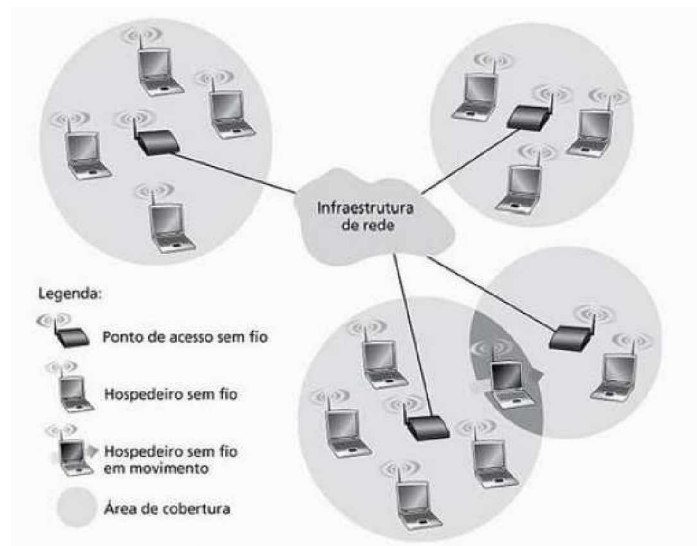


Figura 6 – Exemplo do modo de infra-estrutura de redes sem fio

Fonte: (Kurose, 2010 p.378)

A configuração de uma rede *wireless* é mais complexa do que em uma rede cabeada, pois envolve mais passos e escolhas, como as opções de configuração presentes na interface de administração do ponto de acesso para otimizar a conexão, o tipo de antenas e o sistema de encriptação a ser utilizado.

Já o modo de funcionamento Ad-Hoc, é baseado em redes ponto-a-ponto onde os dispositivos sem fio se comunicam diretamente, sem a necessidade de um ponto de acesso, conforme ilustrado na figura 6. Uma vantagem nesse tipo de operação é a simplificação na troca de arquivos, mas como consequência existe pouca segurança na comunicação entre os dispositivos sem fio (RUFINO, 2005).

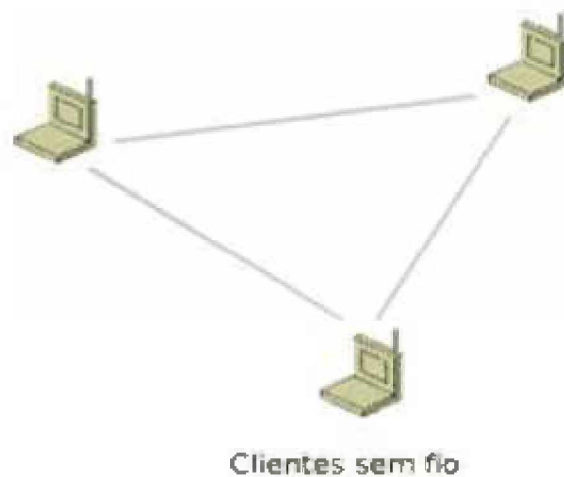


Figura 7 – Rede sem fio no modo Ad-Hoc

Fonte: (<http://technet.microsoft.com/en-us/library/bb457016.aspx>)

2.6 Padrões de comunicação

A padronização da comunicação é necessária para possibilitar a compatibilidade de diferentes fabricantes de equipamentos sem fio, existem diferentes padrões de redes *wireless*, como por exemplo, o *Wireless Fidelity (Wi-Fi)*, *Worldwide Interoperability for Microwave Access (WiMax)*, o *Bluetooth* e outros.

Neste tipo de rede *wireless*, existem os seguintes tipos de redes: *Wireless Local Area Network (WLAN)*, *Wireless Metropolitan Area Network (WMAN)*, *Wireless Wide Area Network (WWAN)*, *Wireless Local Loop (WLL)* e *Wireless Personal Area Network (WPAN)*, como podemos observar na Figura 7.

O *Institute of Electrical and Electronics Engineers (IEEE)* desenvolveram o o “*Wireless Local Area Networks Standard Working Group, IEEE Project 802.11*”, com o objetivo de definir especificações e padrões para as redes sem fio, possibilitando a compatibilidade entre os dispositivos sem fio de diferentes fabricantes. Desde a criação das redes *wireless* os modelos de comunicação foram aprimorando-se em nível de distância e velocidade.

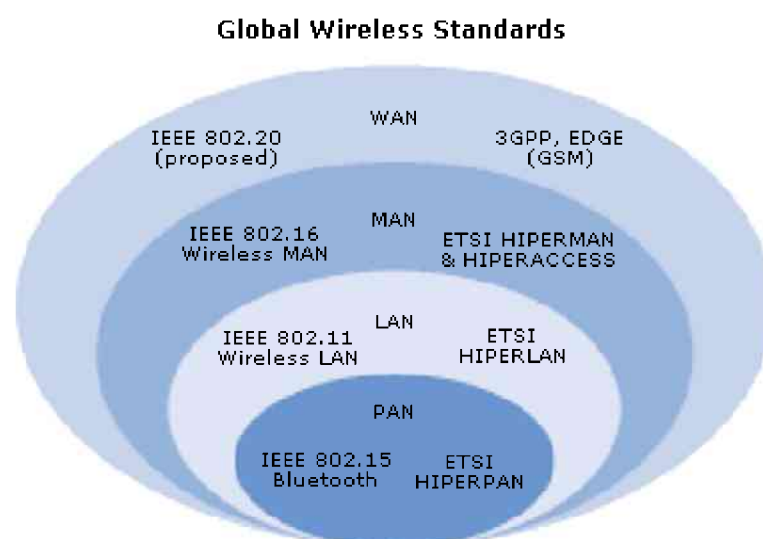


Figura 8 Classificação pela abrangência das redes sem fio.

Fonte: (<http://www.teleco.com.br/tutoriais/tutorialredeswlanII/>)

3 Segurança da informação

A Internet se tornou essencial para as pessoas e instituições como universidades, empresas e órgãos públicos, pois ela possibilita um rápido e fácil gerenciamento e troca de informações, auxiliando nas atividades pessoais, profissionais e sociais dos indivíduos. Porém, é preciso ter cuidado ao se conectar na Internet, pois nela existem muitos “vilões” que tentam colocar os serviços da Internet inoperantes, além de violar a privacidade dos indivíduos e roubar informações sigilosas. Devido a esses fatores, se faz necessário a abordagem de alguns conceitos de segurança com o objetivo de apresentar ao leitor fundamentos envolvidos em segurança de câmeras IP.

Segundo a NBR ISSO/IEC 27002:2005, a segurança da informação é a proteção da informação de vários tipos de ameaças, com o objetivo de minimizar os riscos e maximizar as oportunidades e os retornos do negócio.

3.1 Princípios fundamentais de segurança

A segurança da informação possui três pilares fundamentais que são: a disponibilidade, a integridade e a confidencialidade das informações. Atributos estes que são referenciados na literatura por tríade AIC (Availability, Integrity e confidentiality). Outros atributos importantes relacionados com a segurança da informação são: autenticidade, não repúdio e conformidade (NBR... , 2005).

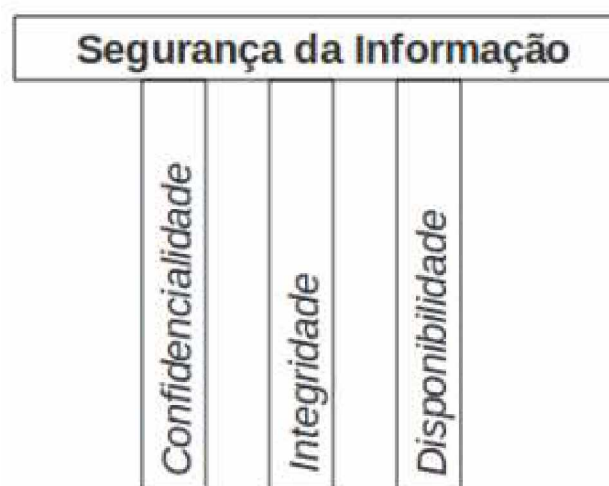


Figura 9 – Princípios fundamentais da segurança da informação.

Fonte: (<https://thiagolucas.wordpress.com/2010/11/18/principios-da-seguranca-da-informacao/>)

3.1.1 Disponibilidade

Disponibilidade é a propriedade que garante que apenas os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR... , 2005).

Os recursos tecnológicos devem ser mantidos em funcionamento, permitindo que os usuários autorizados recuperem de maneira rápida e completamente toda a informação desejada no momento oportuno. Para garantir a disponibilidade da informação, é necessário conhecer os usuários da informação, definir e organizar as formas de disponibilização e de acesso. Algumas medidas são levadas para garantir a disponibilidade, entre elas, destacamos:

- A configuração segura de um ambiente de forma a garantir o êxito da leitura e do armazenamento da informação.
- Cópias de segurança – backup, permitindo outra fonte de acesso, caso a base original não esteja disponível.

3.1.2 Integridade

A integridade é a propriedade que garante que a informação não seja modificada ou destruída sem autorização, que ela permaneça legítima e consistente, ou seja, manter a informação na sua condição original (NBR... , 2005)

A falta de integridade ocorre quando a informação for alterada, destruída, roubada ou falsificada, ela pode ser comprometida tanto com alteração em seu conteúdo quanto no ambiente que lhe oferece suporte.

3.1.3 Confidencialidade

A confidencialidade é a propriedade que assegura a proteção da informação contra o acesso da informação por pessoas não autorizadas, assegurando o valor da informação e evitando divulgações indevidas (NBR... , 2005).

A perda da confidencialidade é a perda do segredo da informação, cada informação possui diferentes graus de confidencialidade, normalmente relacionados aos seus valores e aos impactos causados por sua divulgação indevida. O grau de sigilo é uma classificação atribuída a cada informação, dependendo do seu tipo e do público para o qual se deseja colocar à disposição. Um exemplo de graus de sigilo são: público, sigiloso, restrito e confidencial.

3.1.4 Autenticidade

A autenticidade é a propriedade que trata da legitimidade da informação, garantindo que a informação seja proveniente da fonte anunciada e que não foi alterada ou copiada ao longo de um processo.

A assinatura digital é um dos exemplos de soluções para garantir a autenticidade da informação e a identidade do seu proprietário.

3.1.5 Não-repúdio

O não-repúdio garante que a informação chegará ao destino certo e não será repudiada, com outras palavras, ela garante que o emissor de uma mensagem não poderá negar sua autoria posteriormente.

A assinatura digital é um dos exemplos usados frequentemente como instrumento para garantir o não-repúdio.

3.1.6 Conformidade

A conformidade é a propriedade que garante o cumprimento de leis e regulamentos associados à um tipo de processo (NBR..., 2005).

3.2 Definições de segurança

3.2.1 Vulnerabilidades

As vulnerabilidades são brechas que usuários mal-intencionados utilizam para acessar os conteúdos de um sistema, ocorre na maioria das vezes em sistemas desatualizados.

A NBR ISSO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo que pode ser explorada por uma ou mais ameaças, permitindo a ocorrência de incidentes na segurança da informação.

Existem diversos fatores que estão relacionados diretamente com as vulnerabilidades, como por exemplo fragilidades nos equipamentos, nos processos, nas políticas e nos recursos humanos. Aspectos esses que serão abordados em seguida.

3.2.1.1 Vulnerabilidade Naturais

As vulnerabilidades naturais referem-se as condições da natureza que podem colocar as informações em risco, que podem ser locais propícios a incêndios devido ao tempo seco, locais sujeitos a inundações por estarem próximos a rios, terremotos, maremotos, furacões e desmoronamento.

3.2.1.2 Vulnerabilidade Física

A vulnerabilidade física diz respeito aos ambientes que estão sendo processados as informações, como por exemplo não identificação de pessoas, instalações inadequadas de cabos de energia e de rede, acesso desprotegido às salas de computadores, material inflamável usados na construção.

3.2.1.3 Vulnerabilidades de Hardware

As vulnerabilidades de *hardware* são constituídas por má configuração ou defeitos de fabricação dos equipamentos, possibilitando ataques ou alterações dos mesmos. Essas vulnerabilidades podem originar-se pela falta de configuração e manutenção nos equipamentos, conservação inadequada e firmwares desatualizados.

3.2.1.4 Vulnerabilidade de Software

Caracterizam-se como vulnerabilidade de *software* os pontos fracos das aplicações que possibilitam o acesso indevido ao conteúdo do sistema, geralmente ocorrem devido a configurações e instalações indevidas de programas, falhas de programação e até mesmo no recebimento de e-mails que podem conter códigos maliciosos, causando acesso indevido, perda de dados e vazamento de informações.

3.2.1.5 Vulnerabilidade de Armazenamento

As vulnerabilidades nos meios de armazenamento estão relacionadas como a forma de utilização das mídias em que estão armazenadas as informações, tais como: discos rígidos, disquetes, CD ROM, pen driver e fita magnética.

3.2.1.6 Vulnerabilidade de Comunicação

A vulnerabilidade de comunicação refere-se às fragilidades no tráfego de informações, sejam eles por satélite, cabo ou ondas de rádio. Geralmente ocorre devido à falta de criptografia nas comunicações, no tratamento, leitura e armazenamento das informações e a utilização de protocolos inadequados.

3.2.1.7 Vulnerabilidade Humana

A vulnerabilidade de origem humana é uma das mais preocupantes, já que se refere ao desconhecimento de medidas de segurança, elas podem se originar por diversos motivos tais como: falta de consciência e capacitação técnica na execução segura das atividades rotineiras, erros, omissões, senhas pequenas e fáceis.

3.2.1.8 Vulnerabilidade Organizacional

A vulnerabilidade organizacional refere-se às normas, procedimentos, políticas e todos os aspectos presentes na infraestrutura de controles da organização, como por exemplo a falta de treinamento, a falta de uma política de segurança, falhas em procedimentos internos e falta de planos de contingência.

3.3 Ameaça

Ameaças consiste em agentes que exploram as vulnerabilidades possibilitando a ocorrência de incidentes que comprometem as informações e conteúdo, levando a perda de integridade, disponibilidade e confiabilidade dos mesmos, que como consequência resulta em danos para um sistema ou para uma organização.

As ameaças vêm se tornando cada vez mais comuns devido a automação dos sistemas de processamento e armazenamento de conteúdo, já que as informações estão mais acessíveis e disponíveis para o usuário.

Essas ameaças podem se originar através de uma variedade de eventos, tais como:

Intencionais: são as ações determinadas a causar algum dano como hackers, fraudes, vandalismo, invasão, espionagem e furto de informações;

Involuntárias: ações inconscientes do usuário ocasionando acidentes e erros sem intenção, quase sempre ocorre por vírus presentes em anexos de e-mails.

Naturais: originam-se de fenômenos da natureza como enchentes, terremotos, furacões, queimadas e outros.

3.3.1 Malware

Os *malwares* são códigos maliciosos programados para executar ações danosas em um computador e são utilizados com a finalidade de roubar informações confidenciais, executar golpes, disseminar spams, obtenção financeira e outras (CERT, 2012).

Geralmente os computadores são infectados das seguintes formas:

- Vulnerabilidades existentes, execução de arquivos infectados;
- Acesso a páginas Web com conteúdos maliciosos utilizando navegadores vulneráveis ou desatualizados;
- Auto-execução de mídias removíveis;
- Atacantes que invadem o computador infectando o mesmo com códigos maliciosos.

3.3.1.1 Vírus

O vírus é um programa que executa atividades sem o conhecimento do usuário e se propaga pela rede por meio da inclusão de cópias em outros arquivos. Para que um dispositivo seja infectado por um vírus, é necessário a execução do arquivo infectado, geralmente esses arquivos infectados são passados por e-mail ou mídias removíveis (CERT, 2012).

3.3.1.2 Worm

O *worm* também é capaz de se propagar automaticamente pela rede, os *worms* afetam o desempenho de redes e de computadores pois eles consomem muitos recursos, devido a sua grande quantidade de cópias (CERT, 2012).

3.3.1.3 Bot e Bootnets

Bot é um código malicioso que permite o controle remoto do dispositivo infectado, ele é capaz de se propagar automaticamente, explorando as vulnerabilidades existentes nos programas (CERT, 2012).

O dispositivo infectado por um *bot* é chamado de *zumbi*, pois pode ser controlado remotamente, o invasor consegue enviar diversas instruções para realizar ações maliciosas no computador infectado, tais como: furtar dados do computador infectado, enviar *spam*, realizar ataques de negação.

Botnet é uma rede formada por milhares de dispositivos infectados por um *bot*, quanto maior essa rede, mais potente ela será para realizar ações danosas executadas em conjunto. Alguns proprietários de *botnets* alugam suas redes de computadores *zumbis* para outras pessoas que desejam realizar ações como: ataque de negação de serviço, coleta de informações, envio de *spam* e propagação de código malicioso (CERT, 2012).

3.3.1.4 Spyware

Spyware diz respeito à um programa utilizado para capturar e monitorar as atividades de um usuário em um computador (CERT, 2012).

Alguns exemplos de *spyware* são:

- *Keylogger*: captura e envia as informações do computador para terceiros, como por exemplo as teclas digitadas pelo usuário, podendo facilmente descobrir contas e senhas confidenciais.
- *Screenlogger*: captura imagens da tela quando o usuário clica com o mouse, geralmente utilizados para capturar as senhas de contas de *Internet Banking* onde o usuário geralmente digita a senha em teclados virtuais.

- *Adware*: desenvolvido para apresentar propagandas direcionadas de acordo com a navegação do usuário.

3.3.1.5 Backdoor

Backdoor refere-se a um programa utilizado para garantir acesso remoto ao computador infectado, explorando vulnerabilidades existentes em programas instalados, *softwares* desatualizados e do *firewall*.

3.3.1.6 Trojan

Trojan também chamado de cavalo de troia, caracteriza-se por ser um programa malicioso que executa as funções para as quais foi programado, tais como: instalar outros códigos maliciosos, incluir *backdoors*, desferir ataques de negação de serviço, alterar e apagar arquivos e coletar dados sigilosos do usuário.

3.4 Mecanismos de segurança

3.4.1 Segurança em LANs sem fio

Em redes *wireless*, a criptografia é responsável por bloquear acessos não autorizados, ao adquirir um equipamento *wireless*, é importante entender os principais meios de criptografia disponíveis para proporcionar uma maior segurança.

3.4.1.1 Criptografia de dados

A criptografia consiste na técnica de modificar uma informação para uma forma ilegível, de forma que a informação original possa ser conhecida apenas por seu destinatário, pois o mesmo possui uma chave privada que possibilita a leitura da informação e torna difícil a leitura por alguém não autorizado.

Existem diversas ferramentas de ataques para quebra de criptografia em redes *wireless*, por isso é necessário entender quais são os principais tipos de criptografia para reduzir as possibilidades de um ataque.

Na computação, as técnicas mais conhecidas envolvem as chaves criptográficas, que consiste em um algoritmo responsável por codificar e decodificar informações, onde é necessário que o receptor da mensagem possua uma chave (simétrica ou assimétrica) compatível com a chave do emissor para conseguir extrair a informação, conforme ilustrado na figura 6.

A chave simétrica, também chamada de chave privada ou criptografia tradicional, é um método eficiente em aplicações de uso limitado, onde ocorre uma preparação antecipada tanto para o transmissor quanto para o receptor, para a utilização da chave. Foram

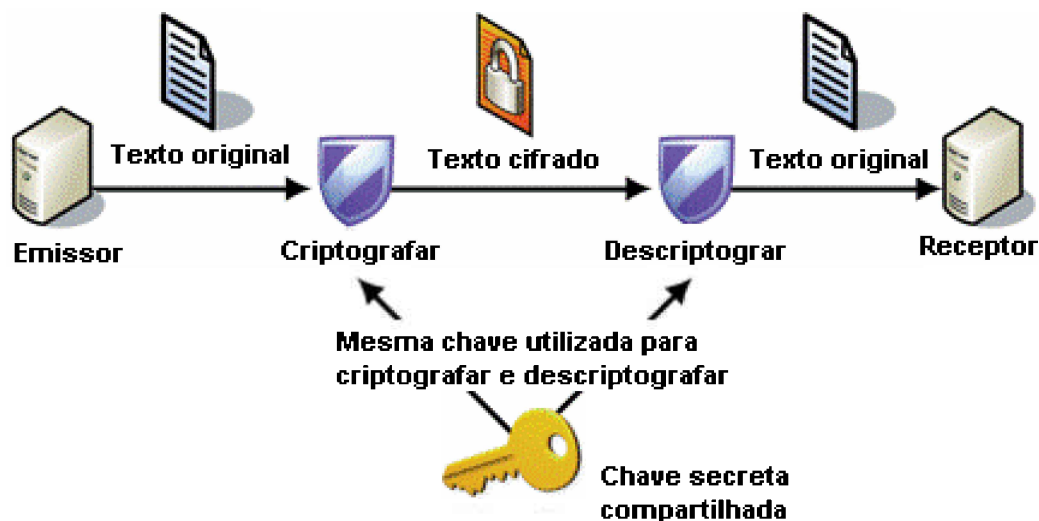


Figura 10 Processo de criptografia simétrica.

Fonte: (<http://www.devmedia.com.br/criptografia-conceito-e-aplicacoes-revista-easy-net-magazine-27/26761>)

desenvolvidos vários algoritmos de criptografia com chaves simétricas, os mais comuns são o DES, o IDEA e o RC.

DES (*Data Encryption Standar*): foi criado em 1977 pela IBM, utiliza de chaves de 56 bits e apesar de permitir até 72 quatrilhões de combinações foi quebrado por meio de força bruta.

IDEA (*International Data Encryption Algorithm*): foi criado por James Massey e Xucjia Lai em 1991, composto por um algoritmo que possui estrutura parecida com a do DES e utiliza chave de 128 bits.

RC (*Ron's Code ou Rivest Cipher*): criado por Ron Rivest, utiliza chaves de 8 a 1024 bits, possui várias versões (RC2, RC4, RC5 e RC6).

Já a chave assimétrica ou chave pública, foi desenvolvida em 1976 por Diffie e Hellman, o termo “assimétrica” vem do uso de diferentes chaves para realizar funções opostas, nesse modelo, cada participante deve possuir duas chaves diferentes, sendo uma chave pública e outra chave privada. A chave pública é usada, por exemplo, para criptografar a informação ou verificar a assinatura digital. Já a chave privada é usada para descriptografar uma informação ou criar uma assinatura digital.

O algoritmo utilizado até hoje é o RSA e foi inventado por três professores chamados Rivest, Shamir e Adleman, o algoritmo gera dois pares de números, onde uma informação criptografada com o primeiro par só pode ser descriptografada com o segundo par.

3.4.1.2 Wired Equivalent Privacy (WEP)

A popularização e crescente utilização de redes sem fio proporcionou mobilidade e praticidade para os usuários, mas também proporcionou uma maior preocupação com a segurança dessas redes, e por isso foram criados os protocolos de segurança, que são desenvolvidos e atualizados constantemente.

O WEP foi o primeiro protocolo de segurança utilizados nas redes sem fio, este protocolo utiliza o algoritmo RC4 para criptografar os pacotes. Existem problemas neste protocolo pois caso seja necessária a troca da chave, o processo pode ser muito trabalhoso, já que é compartilhado entre todos os participantes de uma determinada rede uma chave única e estática (RUFINO, 2005).

Foram achadas algumas vulnerabilidades e falhas no protocolo WEP após estudos e testes, o que fez com que o WEP perdesse sua credibilidade devido à alguns fatores, como por exemplo:

Tamanho de Chave: inicialmente o WEP possuía uma chave estática de apenas 40 bits, o que possibilitava que essas chaves fossem quebradas por “força bruta”, então foi desenvolvido o WEP2 com chave estática de 104 a 232 bits para solucionar esse problema.

Reuso de chaves: os 24 bits do vetor de inicialização permitem cerca de 16,7 milhões de vetores diferentes, esse número é relativamente pequeno em termos de volume de rede, fazendo com que ocorra um considerável número de repetição de chaves, que por consequência afeta a confidencialidade dos dados. Devido a essa falha, poderosos ataques são realizados em redes sem fio que ainda utilizam a criptografia WEP.

Gerenciamento de chaves: a chave utilizada pelos dispositivos não pode ser trocada dinamicamente pois o WEP não utiliza algum protocolo para o gerenciamento de chaves, o que dificulta o gerenciamento das redes.

3.4.1.3 Wi-fi Protected Access (WPA)

O WPA, também chamada de WEP2 por ser considerado um WEP melhorado, é um protocolo de comunicação via rádio, sua primeira versão surgiu através da necessidade de tratar algumas vulnerabilidades do WEP afim de aumentar a segurança das redes sem fio, foi criado por membros do IEEE e da *Wi-Fi Aliança*.

O WPA teve algumas vantagens com relação ao WEP, como o uso do protocolo de chave temporária *Temporal Key Integrity Protocol* (TKIP) que possibilita a criação automática de chaves por pacotes, melhorando na criptografia dos dados, a extensão de 24 para 48 bits de chave permitindo cerca de 16 milhões de chaves distintas a mais do que o WEP além de possuir uma função de detecção de erros (RUFINO, 2005).

Mesmo com todas as melhorias do WEP para o WPA, foram descobertas algumas

falhas de segurança que levou a criação do WPA 2 Personal.

3.4.1.4 Wi-fi Protected Access - Personal

Com os problemas de segurança das redes wireless, surgiu a necessidade de criar um modo de criptografia forte e intuitiva, então criou-se o WPA-PSK (WPA – Pre Shared KEY), também conhecido como WPA2-PSK ou WPA Personal. A chave de acesso protegido Wi-Fi é uma forma previamente compartilhada entre o access pointer e seus clientes, ou seja, é um mecanismo de segurança que valida e autentica os usuários de uma rede LAN sem fio (WLAN) ou conexão Wi-Fi. O WPA-PSK funciona configurando uma senha de oito a 63 caracteres. Ele então gera uma chave de 256 caracteres levando em consideração a senha, o access pointer e as credenciais do nó de conexão, então essa chave de acesso é compartilhada para os dispositivos afim de criptografar e decodificar o tráfego de rede. O WPA 2 Personal é muito indicado para ambientes domésticos com poucos usuários.

3.4.1.5 Wi-fi Protected Access - Enterprise

O WAP Enterprise foi projetado para redes corporativas e requer um servidor de autenticação, o que necessita de uma configuração mais complexa levando à um nível de segurança maior. Na autenticação são utilizados uma infraestrutura complementar formada por vários tipos de protocolos de autenticação extensível (EAP). O seu funcionamento consiste na verificação da base de dados do servidor de autenticação, se o cliente solicitante possui as credenciais válidas, para então poder autenticá-lo e enviá-lo uma chave chamada Master Session Key (MSK), conforme é ilustrado na figura 8.

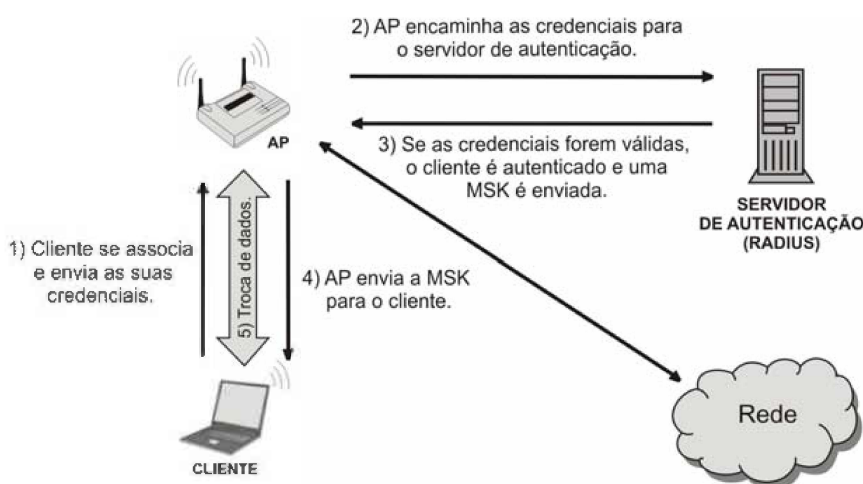


Figura 11 – Processo de autenticação com servidor.

Fonte: (<http://www.unibratce.com.br/jornadacientifica/diretorio/UFPEAGL.pdf>)

3.4.1.6 Protocolo de Autenticação Extensível - EAP

O Protocolo de Autenticação Extensível (Extensible Authentication Protocol - EAP) é responsável por criar uma comunicação segura entre o servidor de autenticação e o cliente, por meio de um canal lógico onde as credenciais irão trafegar.

Ele é um protocolo que permite vários métodos de autenticação, com as modalidades de autenticação por certificados de segurança ou por senhas.

Os exemplos dos métodos de autenticação do EAP por certificado de segurança são:

EAP-TLS: possui a autenticação mútua, ou seja, exige a instalação de certificados de segurança nos servidores e nos clientes utilizando o protocolo TLS (*Transparent Layer Substrate*).

EAP-TTLS: parecido com o EAP-TLS, mas o certificado de segurança é instalado apenas no servidor, a autenticação do cliente por parte do servidor ocorre com a utilização de outro método como PAP, CHAP, MS-CHAP ou MS-CHAP V2.

PEAP: foi desenvolvido pela Microsoft, Cisco e RSA Security, é parecido com o EAP-TTLS pois também requer certificado de segurança apenas no servidor.

EAP-MD5: requer um usuário e senha para a autenticação. A senha é cifrada através do algoritmo MD5, não há como autenticar o servidor e não gera chaves WEP dinâmicas. Esse método não possui um bom nível de segurança, pois pode sofrer ataques de força bruta.

LEAP: suporta chaves WEP dinâmicas e usa nome de usuários e senha, é um método proprietário da Cisco e por isso exige que os equipamentos sejam da Cisco.

EAP-SPEKE: permite um serviço de autenticação mútua com o compartilhamento de uma senha secreta entre o cliente e o servidor, com a utilização do método SPEKE (*Simple Password-authenticated Exponential Key Exchange*).

3.4.2 Honeypot

É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

3.4.3 FIREWALL

Em português parede de fogo, consiste em uma barreira de proteção que filtra todo o fluxo de dados da rede bloqueando os conteúdos maliciosos, garantindo a integridade e a confidencialidade dos dados.

4 Câmeras IP

4.1 Introdução a câmeras IP

A câmera IP, também conhecida como câmera de rede, consiste em uma câmera com um computador integrado, ela possui seu próprio endereço IP e pode ser colocada onde houver conexão de rede. Seus principais componentes são: o sensor de imagem, a lente, a memória, um ou mais processadores e portas de entrada e saída ([TECNOLOGIA... , 2013](#)).

A memória armazena o *firmware* da câmera IP e as gravações locais de sequências de vídeos.

Os processadores são responsáveis pelo processamento digital das imagens, compactação das imagens e funções de conexão de rede.

As portas de entrada e saída possibilitam conexões com dispositivos externos como alarmes, relés e sensores.

A câmera IP possibilita o envio das gravações por uma rede IP para a visualização ao vivo, além de capturar vídeo, as câmeras IP possuem funções inteligentes, como detecção de áudio e detecção de movimento. Conforme o manual da fabricante de câmeras IP chamada Axis, as imagens capturadas podem ser enviadas em formatos como vídeo H.264, MPEG-4 ou Motion JPEG ([TECNOLOGIA... , 2013](#)).

4.1.1 Primeira câmera IP

A primeira câmera IP foi criada em 1996 pela empresa Axis Communications fundada em 1984 por Martin Gren, Mikael Karlsson e Keith Bloodworth. A câmera denominada Axis Neteye 200 digitalizava as imagens analógicas e transmitia pela rede usando o protocolo TCP/IP, ela trabalhava com apenas 3 frames por minuto, era uma revolução na época, pois permitia o acesso remoto em redes já instaladas e contriuiu para uma economia de milhares de dólares em projetos industriais por permitir o monitoramento remoto.

4.1.2 Tipos de câmeras IP

As câmeras IP são classificadas com base nas necessidades e no seu uso previsto: uso interno, externo ou ambos e são categorizadas como fixas, domes fixas, PTZ e domes PTZ.

Câmera IP fixa

A câmera IP fixa possui seu campo de visão fixo, ela pode ter uma lente fixa ou de foco variável, onde a direção para qual a câmera é apontada captura as imagens claramente visíveis (TECNOLOGIA..., 2013).



Figura 12 – Câmera IP externa fixa com infravermelho

Fonte: ([http : //biblioteca.omegatecnologia.com/busca_artigo/542/artigos/99/entendendo-e-conhecendo-cameras-e-seguranca.html](http://biblioteca.omegatecnologia.com/busca_artigo/542/artigos/99/entendendo-e-conhecendo-cameras-e-seguranca.html))

Câmera IP domo fixo

A câmera IP tipo domo fixo, consiste em uma câmera dentro de uma pequena cúpula, suas vantagens estão no seu visual discreto que dificulta a percepção sobre qual direção a câmera está apontando e por serem projetadas em caixas de proteção resistentes, geralmente essa câmera é fixada no teto ou na parede (TECNOLOGIA..., 2013).

Câmera PTZ ou dome PTZ

A câmera PTZ ou a dome PTZ podem ser instaladas no teto ou em uma parede, elas possuem recursos de aproximar ou afastar a imagem (*zoom in/out*) e se movimentar na vertical e na horizontal (*pan/tilt*), esses recursos permitem um monitoramento extenso com uma única câmera, normalmente essas câmeras são utilizadas com a presença de um operador que analisa as imagens em tempo real, seus comandos são enviados através do cabo de rede. Mesmo que essas câmeras possuam funções semelhantes, a câmera dome PTZ se diferencia por possibilitar o monitoramento de uma área maior pelo fato de ter uma maior flexibilidade em movimentar-se 360° continuamente na horizontal e normalmente 180° na vertical (TECNOLOGIA..., 2013).



Figura 13 – Câmera IP dome fixa

Fonte: (<http://www.mondoplast.ro/Camera-IP-Dome-fixa-Full-HD-H-264-Real-Time-Planet-ICA-HM131R-pgft-4963>)



Figura 14 – Câmera IP PTZ

Fonte: (<https://www.axis.com/rs/en/products/axis-p54-series>)

4.1.3 Componentes internos de uma câmera IP

Conforme a figura 15, uma câmera IP possui os seguintes componentes:

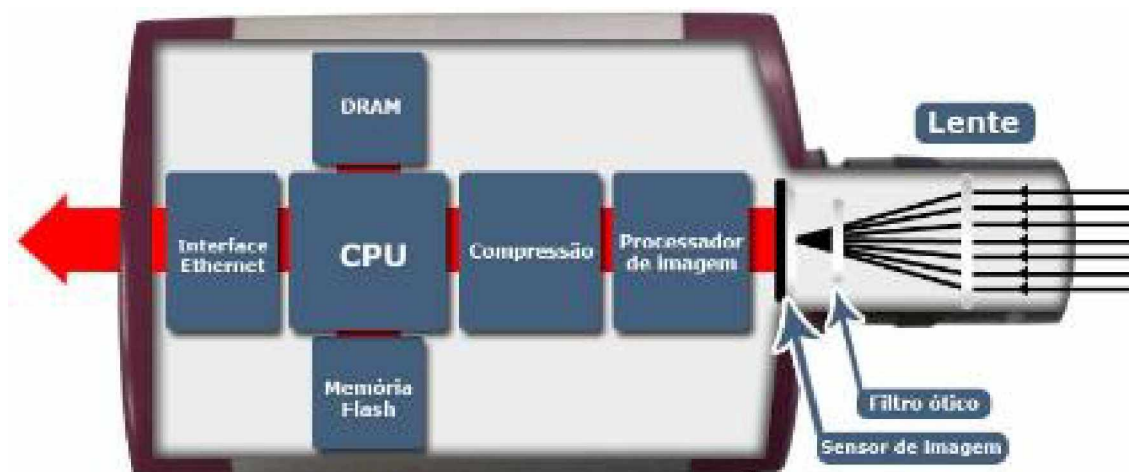


Figura 15 – Câmera IP PTZ

Fonte: <http://www.ebah.com.br/content/ABAAABAUQAB/projeto-cftv-digital>

- *Lente*: focaliza a imagem sobre o sensor de imagem, ou seja, direciona a luz capturada para o sensor interno (CMOS);
- *Filtro*: filtra a luz antes de chegar no sensor;
- *Sensor de imagem*: converte a imagem em sinais elétricos, o que possibilita que estes sinais sejam comprimidos e transmitido pela rede;
- *Processador de imagem*: esse componente processa as imagens vindas do sensor e realiza algumas melhorias quando necessário, para então passar para o circuito final que irá processar e enviar as imagens pela rede.
- *Compressor de imagem*: usa um algoritmo para comprimir as imagens;
- *CPU, memória flash e memória RAM*: em conjunto elas controlam a comunicação da câmera com a rede e o servidor de web interno, esse conjunto foi projetado para aplicações de rede;
- *Entrada e saída de áudio, alarme e cartão SD*: essas entradas geralmente estão localizadas na parte traseira da câmera
- *Interface Ethernet*: envia imagens simultaneamente para os usuários.

4.1.4 Vantagens das câmeras IP

A câmera IP possui diversas vantagens quando comparado com a câmera analógica, sua diferença básica está na digitalização das imagens, ou seja, transformar para o formato digital facilitando na transferência e no armazenamento do arquivo pela rede e pela Internet.

O processo de digitalização em uma câmera IP ocorre diretamente na câmera antes mesmo de ser enviada para um gravador, essa digitalização na própria câmera IP possibilita a utilização de recursos de inteligência.

A câmera IP possui uma fácil instalação, não exige o investimento de uma nova estrutura de cabeamentos, sendo necessário apenas um cabo por câmera para o fornecimento de energia e transporte dos dados.

Entrada e saída de alarmes, áudio e cartão SD, o que permite conectar vários dispositivos para aperfeiçoar ainda mais a vigilância, como por exemplo microfone externo, auto falante, cartão de memória, alarme e dispositivos externos para sinalização sonora e luminosa.

Um sistema de vigilância composto por câmeras IP, possui um custo menor do que um sistema com câmeras analógicas, isso acontece devido à economia com o uso de cabos coaxiais e cabos de fibra que não são utilizados com as câmeras de rede, possibilitando um reaproveitamento da infraestrutura de rede já existente.

Existe a possibilidade de dupla alimentação em paralelo, utilizando uma fonte tradicional e através do cabo de rede, o que impede que a câmera pare de funcionar mesmo quando o cabo de rede é cortado ou desconectado.

Outra vantagem é a comunicação bidirecional onde os usuários podem ter acesso direto à câmera e utilizar seus recursos, como por exemplo: ver as imagens, ouvir áudio através do microfone da câmera, transmitir áudio através do auto falante presente na câmera, gerenciar a câmera pelos comandos de PAN/TILT e ZOOM IN/OUT entre outros.

As câmeras IPs possuem uma inteligência embarcada, possibilitando uma análise inteligente dos vídeos afim de detectar possíveis alterações para tomar uma ação pré-programada, como por exemplo: detecção de movimento, detecção de rosto, detecção de placas de veículos, contagem de pessoas, detecção de áudio entre outros.

As câmeras analógicas possui pouca resolução das suas imagens, geralmente não passam de 5 megapixels, o que dificulta na identificação de rostos e placas em uma imagem capturada, já as câmeras IP possibilita uma melhor qualidade e resolução das imagens capturadas pois elas possuem uma capacidade maior de megapixels e suas imagens são digitalizadas apenas uma vez, sem realizar conversões desnecessárias, evitando a perda de qualidade, o que permite capturar imagens claras de pessoas e objetos.

A criptografia dos dados é outra vantagem presente nas câmeras IPs pois ela garante mais segurança das imagens capturadas, já que os dados só podem ser descritos no seu destino, o que torna inútil a interceptação dos dados.

Os sistemas de vigilância de rede, possibilita a utilização de muitas câmeras IP e codificadores de vídeo na mesma rede para receber e transmitir os dados, essa caracte-

ística permite incluir mais dispositivos no sistema de vigilância, sem nenhuma alteração significativa ou de alto custo na infraestrutura da rede. Diferente de um sistema analógico onde é necessário um cabo coaxial ligando cada câmera com a estação de gravação ou visualização.

O grande número de câmeras em um sistema de vigilância ocasiona em um grande volume de vídeos armazenados, as câmeras de rede IP possuem recursos de análise que reduzem gravações desnecessárias. Esses recursos consistem em funções de detecção de movimento, detecção de áudio, envio de notificações por mensagem, acionamento de alarmes, de luzes e portas quando ocorrer eventos anormais. Essas funcionalidades são configuradas conforme a necessidade do projeto e por meio da interface de usuário do fabricante das câmeras ou por softwares de gerenciamento de vídeo facilmente encontrados na Internet.

Uma das maiores vantagens das câmeras IP, e que requer muita atenção para garantir a segurança e privacidade das imagens, consiste na acessibilidade remota, onde mais de um usuário autorizado possa acessar remotamente as imagens capturadas pelas câmeras ao vivo ou gravadas, em qualquer lugar com acesso à Internet e a qualquer momento.

4.1.5 Diretrizes para um projeto de vigilância IP

Como foi escrito anteriormente, existe uma variedade de câmeras IP que são adequadas para cada caso específico. Primeiramente é necessário analisar os objetivos da instalação das câmeras de vigilância para definir os requisitos ideais para o projeto, tais como:

- Objetivo da vigilância: O projeto visa o capturar imagens panorâmicas de um amplo ambiente ou imagens mais detalhadas para capturar rostos, placas de carro e objetos(TECNOLOGIA... , 2013).
- Área da cobertura: determinar a área de cobertura e sua extensão para decidir a quantidade e o tipo de câmeras mais adequadas, por exemplo, uma área pode ser monitorada por várias câmeras IP fixas ou por um número reduzido de câmeras IP PTZ(TECNOLOGIA... , 2013).
- Ambiente interno ou externo: em ambientes externos é necessária uma câmera com maior sensibilidade à luz, devido a iluminação do ambiente que pode variar durante o dia e a noite, uma câmera infravermelha seria mais adequada para essas ocasiões(TECNOLOGIA... , 2013).
- Vigilância explícita ou discreta: existem projetos de vigilâncias explícitos que o objetivo é que as pessoas vejam as câmeras e saibam qual área está sendo monitorada, geralmente com o uso de câmeras IP fixas. Já para os projetos com objetivos de uma

vigilância discreta, câmeras IP dome seriam mais adequadas, já que elas são menores e possuem modelos fumê que impossibilita o indivíduo que está sendo monitorado em saber para onde a câmera esta focando(TECNOLOGIA..., 2013).

- Compactação: essa técnica é utilizada para reduzir dados redundantes do vídeo capturado, a fim de otimizar a transmissão e o armazenamento dos dados pela rede. Os padrões de compactação mais utilizados nas câmeras IPs são: Motion JPEG, MPEG-4 e o mais recente H.264(TECNOLOGIA..., 2013).
- Funções de rede: é essencial considerar quais funções de rede devem compor às câmeras do projeto, entre as considerações estão: criptografia HTTPS para criptografia de fluxos de vídeo antes que eles sejam enviados pela rede, PoE, filtragem de endereços IP que concede acesso aos IPs dos dispositivos definidos, IEEE802.1X para controlar o acesso a uma rede; IPv6; e funções wireless(TECNOLOGIA..., 2013).
- Largura de banda e armazenamento: a largura de banda utilizada para transmissão e armazenamento dos vídeos depende diretamente da qualidade dos mesmos, ou seja, quanto maior a qualidade, maior largura de banda e espaço para armazenamento serão necessários. A qualidade da imagem é determinada por diversos fatores, entre eles estão:
 - Resolução da imagem: que consiste no tamanho da imagem em pixels. Em CFTV existem diferentes resoluções como: VGA, SVGA, D1, CIF 2CIF 4CIF. Porém, as nomenclaturas que os usuários finais mais conhecem são: HD, Full HD, 4k, Mega Pixel.
 - Taxa de quadros por segundo: também chamado de FPS, consiste no número de frames gravados por segundo, quanto maior o número de imagens gravadas por segundo, melhor será o vídeo pois a imagem será mais contínua e consequentemente necessitara de um maior uso de banda e armazenamento.
 - Algoritmo de compressão (CODEC): é um algoritmo matemático utilizado para comprimir o vídeo capturado, reduzindo seu tamanho para ser transportado e armazenado. Em CFTV o algoritmo mais utilizado é o H.264.
 - Gravação contínua ou por evento: a câmera pode ser programada para gravar continuamente ou quando houver um evento, como por exemplo detecção de movimentos ou eventos gerados por sensores conectados à câmera. Uma câmera programada para gravar apenas em determinados eventos, ela irá armazenar os vídeos somente no período específico do evento, auxiliando na redução do espaço de armazenamento e na busca de ocorrências.
 - Quantidade de movimento: esse critério varia de um ambiente para outro, em um ambiente com muita movimentação de carros e pessoas, a câmera terá

que processar mais informações, o que custa mais recursos para transmitir e armazenar o vídeo.

4.2 Ameaças e vulnerabilidade em câmeras IP

Os circuitos de monitoramento por câmeras IP estão cada vez mais presentes nas residências e empresas no mundo inteiro, isso ocorre devido à evolução desses equipamentos, cada vez mais eficientes, acessíveis e fáceis de configurar.

Qualquer dispositivo conectado a uma rede IP pode sofrer ataques e invasões de *hackers* e vírus, o grande número de câmeras IP conectadas a Internet pode se tornar um problema grave, já que a segurança desse dispositivo é limitada, mesmo para os equipamentos de marcas de renome. A era da Internet das Coisas vem contribuindo para que os atacantes utilizem desse gigantesco número de equipamentos conectados à Internet para construção de *botnets*, já que a maioria das câmeras IP não possuem controles de segurança adequados e são facilmente acessíveis via *telnet*. Assim, os ataques às câmeras IP se resumem em três passos simples: buscar dispositivos vulneráveis, instalar malware e construir uma *botnet*.

Existem diversas botnets prontas para realizar grandiosos ataques de negação de serviço, abaixo está listado as três mais importantes já registradas:

BASHLITE é um dos malwares mais populares que infecta dispositivos baseados em Linux para lançar ataques DDoS. Foi relatado que BASHLITE é responsável por escravidar mais de 1 milhão de dispositivos da Internet das coisas, constituindo principalmente de câmeras IP e DVRs habilitados para a Internet.

Ele é capaz de lançar ataques de até 400 Gbps, a maioria dos ataques BASHLITE são simples UDP, TCP e ataques HTTP. Ele infecta os dispositivos acessando a telnet por força bruta ou usando credenciais padrões dos fabricantes. A maioria dos dispositivos infectados estão localizados em Taiwan, Brasil e Colômbia.

Mirai é um dos mais predominante botnet nos últimos tempos, o nome Mirai significa "futuro" em japonês, ele tem a capacidade de infectar mais de 4000 dispositivos da Internet das coisas por hora e atualmente estima-se ter pouco mais de meio milhão de dispositivos infectados. Mirai botnet é famoso por ter batido o recorde de ataque DDoS de 1.1Tbps com 148000 dispositivos, principalmente câmeras de CCTV, DVRs e roteadores domésticos. Seu potencial pode chegar até 1,2 Tbps (DUCKLIN, 2016).

Seu código fonte foi publicado por seu suposto autor Paras Jha na comunidade Hackforums como open-source. Desde o lançamento do código-fonte do Mirai, o número de dispositivos infectados da Internet das coisas aumentou de 213.000 para 483000 em apenas duas semanas (DUCKLIN, 2016).

Com base nos endereços IP pode-se identificar que os dispositivos infectados pelo Mirai estão distribuídos em mais de 164 países com maiores densidades no Vietnã, Brasil, Estados Unidos, China e México (MICHAEL, 2017).

Ele chamou a atenção em setembro de 2016 depois do ataque DDoS contra o site de segurança KrebsOnSecurity.com que atingiu 620 Gbps (KREBS, 2016b). Depois do ataque ao site krebsonsecurity.com ele foi usado no ataque da empresa francesa de hospedagem OVH, que atingiu cerca de 1Tbps (THE..., 2016).

Persirai é o novo botnet da Internet das Coisas, detectado pela Trend Micro como ELF PERSIRAI A. Segundo especialistas da Trend Micro, o botnet atacou mais de mil modelos de câmeras IP de uma fabricante chinesa e foi detectado que cerca de 120 mil câmeras IP estão vulneráveis ao Persirai (MICHAEL, 2017).

Após o invasor conseguir logar na interface vulnerável, ele executa um comando que força a câmera a acessar um site de download para baixar e executar o malware do Persirai, e com comandos no servidor, a câmera IP começa a atacar outras do mesmo modelo automaticamente, conforme imagem a seguir acrescentada pela Trend Micro.

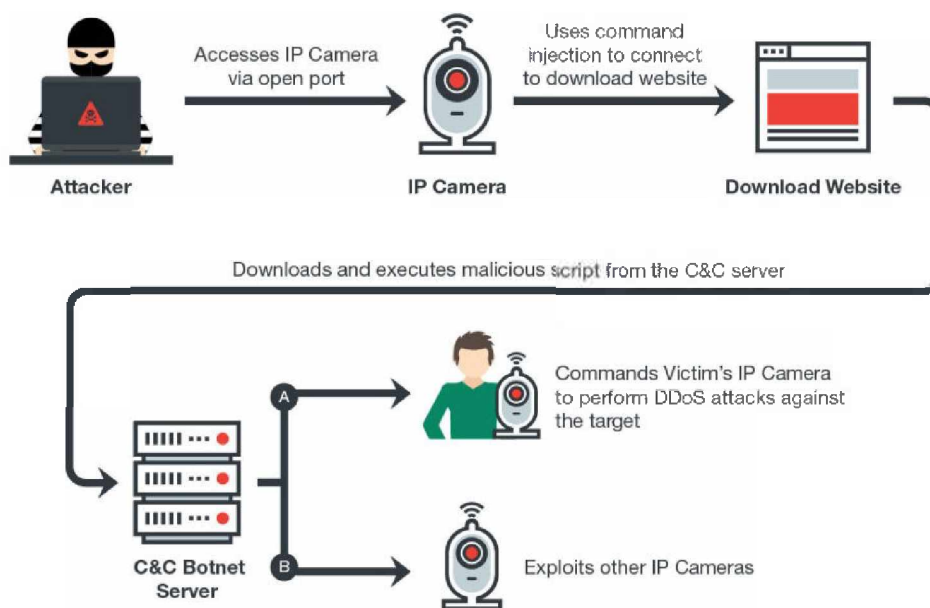


Figura 16 – Fluxo de infecção de ELF PERSIRAI A

Fonte: (<http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>)

Existem diversas vulnerabilidades nos dispositivos de vídeo-monitoramento conectados à rede, muitas delas ocorrem devido à falta de consciência dos usuários, fabricantes e instaladores. Essas brechas merecem uma atenção maior pois, quando exploradas, per-

mitem que um invasor não autenticado tenha o controle total dos recursos dos dispositivos conduzindo a uma perda total de confidencialidade, integridade e disponibilidade.

Por exemplo, o invasor pode visualizar as imagens da câmera, controlar a funcionalidade e operação da câmera, fazer download dos arquivos do servidor via FTP, e usar os dispositivos para outras ações mal-intencionadas como ataques DDoS.

Atualmente o número de comércios e residências que possuem câmeras IP aumentou muito, devido à evolução e barateamento desses dispositivos. Com a crescente demanda de clientes surgem muitos fabricantes que não se preocupam com as vulnerabilidades de seus dispositivos comercializados, esses fabricantes simplesmente vendem uma quantidade massiva de dispositivos por todo o mundo sem oferecer alguma atualização de segurança do firmware que minimize suas vulnerabilidades, nem se quer uma simples função de tornar obrigatório a alteração das senhas padrões das câmeras IP.

Facilmente encontramos lojas que vendem câmeras IP com preços muito acessíveis, porem a aquisição desses equipamentos podem se tornar uma dor de cabeça, visto que muitos desses equipamentos não possuem marca e nenhuma informação do fabricante, nem seque um número telefônico para um suporte, o que impossibilita qualquer atualização do firmware para solucionar eventuais problemas de ataques.

É fato que os grandes fabricantes se preocupam mais em minimizar as vulnerabilidades de seus produtos para zelar seu nome. Porém, não existe nenhum produto totalmente seguro, independente de qual for o fabricante, grandes marcas como Samsung, Sony, Axis, Cisco e Bosch também possuem problemas de segurança. Infelizmente há profissionais que acreditam que não precisam se preocupar com segurança quando utilizam os produtos dessas grandes marcas, tornando esses dispositivos alvo fácil para ataques e invasões.

A falta de um conhecimento profundo dos técnicos e instaladores facilita a invasão dos dispositivos na rede, principalmente devido a possibilidade de acesso remoto ao cliente, muitos desses profissionais não se preocupam com questões de segurança como protocolos e nem se quer alteram a senha padrão do dispositivo.

É muito raro um usuário final que atualiza o firmware de suas câmeras IPs, uma vez instaladas elas ficarão por muito tempo sem as atualizações que minimizam problemas de segurança que são descobertos por pessoas mal-intencionadas, isso se dá por falta de consciência dos usuários finais em pesquisar por atualizações no site dos fabricantes e por quererem economizar com o custo de manutenção desses equipamentos.

As credenciais padrão constituem um grave e frequente problema nos sistemas de vigilância compostos por câmeras IP, quando os usuários não alteram os credenciais padrões definidas pelos fabricantes um atacante pode ter acesso privilegiado ao dispositivo, infectando-o com um malware para realizar ataques DDoS e executar outras atividades

maliciosas como baixar e carregar arquivos do servidor via FTP e assistir as imagens capturadas pela câmera via RSTP.

Conforme a figura 13, o ano de 2017 bateu recordes em vulnerabilidades reportadas ao cvedetails.com, muitas dessas vulnerabilidades já foram corrigidas, porém é necessário que o usuário atualize o *firmware* de sua câmera para poder corrigir as vulnerabilidades presentes em seu dispositivo.

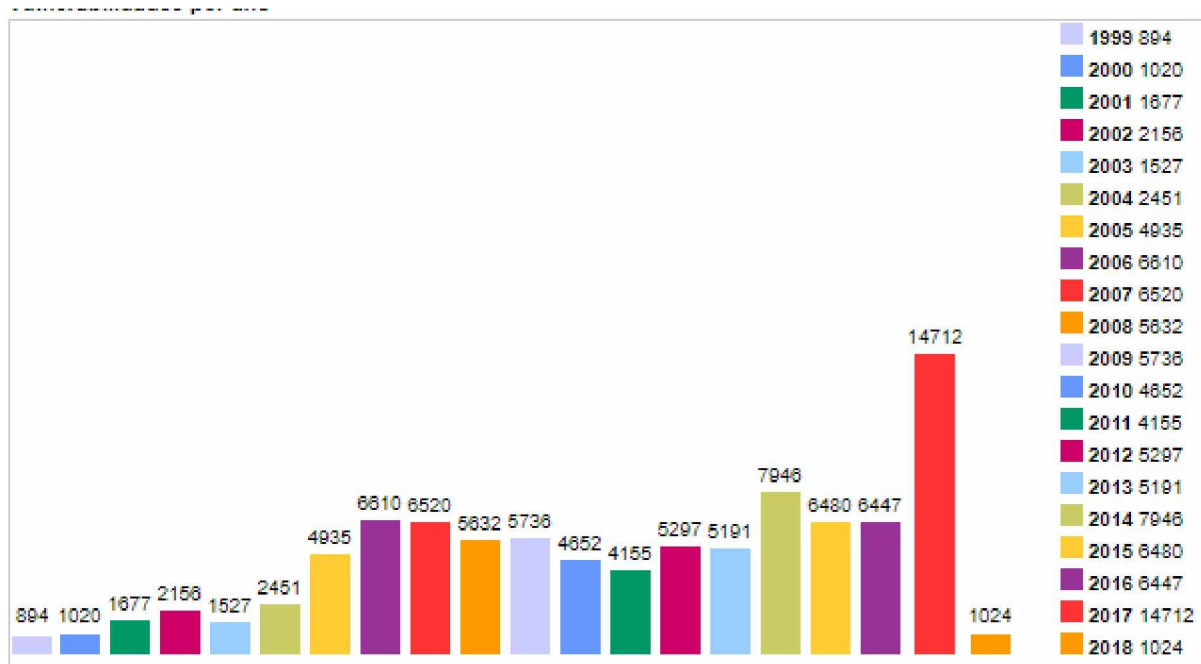


Figura 17 – Vulnerabilidades por ano

Fonte: (<https://www.cvedetails.com/browse-by-date.php>)

O software dos dispositivos de uma grande fabricante de câmeras IP fornece um recurso crítico de configuração de permissões, esses recursos críticos são facilmente acessados por injeção de comandos, o que concede ao invasor privilégios de root possibilitando-o a ler, modificar e realizar qualquer ação permitida pelas credencias de administrador (MICHAEL, 2017).

De acordo com estudos realizados pela F-Secure, diversos fabricantes atribuem permissões incorretas para o script de inicialização dos dispositivos, a cadeia de execução de inicialização de vários modelos de câmeras de uma grande fabricante é: `/sbin/init -> /etc/inittab -> /etc/init.d/rcS -> /etc/init.d/S90init -> /mnt/mtd/boot.sh`. O problema é que o script `/mnt/mtd/boot.sh` é alterável e armazenado em memória flash, permitindo que qualquer usuário consiga acessá-lo e modificá-lo, e que essas alterações sejam reinicializadas no sistema, pois sempre quando o sistema é ligado, o arquivo é executado. (MICHAEL, 2017).

Muitos usuários acreditam que o firewall restringe acesso ao dispositivo, no entanto,

apenas protege o acesso à interface do usuário da web, nas portas 88 e 443. Então o firewall não impede de um invasor acessar serviços com FTP, RTSP e telnet (HENRIQUE, 2017).

Uma vulnerabilidade simples de se resolver que muitas fabricantes não deram a devida atenção é em impor uma restrição para múltiplas tentativas de login, restringindo o usuário de tentar fazer login diversas vezes com credenciais incorretas, possibilitando ataques de força bruta contra as credenciais de login.

Para piorar, as pessoas mal-intencionadas documentam as vulnerabilidades encontradas nos dispositivos de diversas marcas e modelos, divulgando de forma colaborativa todos os detalhes e brechas encontrados para facilitar que outras pessoas invadem os sistemas.

4.2.1 Ataques

- A violação de acesso é uma das ameaças mais comuns em se tratando de câmeras IP, essa ameaça refere-se quando seus serviços e elementos de rede são acessados indevidamente. Normalmente esse ataque acontece como primeiro passo para a realização de outros ataques.
- Interceptação de senha entre cliente e servidor (man-in-the-middle): esse ataque é bem comum e consiste quando o atacante se posiciona entre o cliente e o servidor dentro de uma rede, para interceptar uma cópia da senha de acesso enviada do cliente para o servidor, então independente se a senha for grande e complexa, o atacante poderá receber a senha.
- Ataque de força bruta (tentar uma sequência de possíveis senhas) e ataque de dicionário (tentar uma sequência de palavras como senhas): para a realização desses ataques, os hackers utilizam programas que enviam rapidamente uma sequência de senhas até acertar a senha de acesso, para ser mais rápido e melhorar as chances de acertos, são utilizados computadores com alto poder de processamento capazes de tentar milhares de combinações em apenas um minuto e dicionários com combinações de caracteres, existem vários tipos de dicionários e eles se diferenciam por vários fatores, tais como: idioma, região, costumes, idade e nomes.
- Exploração de vulnerabilidade em serviços (como o WebServer): esse tipo de ameaça é realizado por pessoas com um conhecimento mais profundo em programação, com habilidades de desenvolvimento de softwares e conhecimentos dos sistemas operacionais e dos serviços que são executados dentro de cada dispositivo. Para isso, o hacker adquire um dispositivo como uma câmera IP ou um DVR para estudar os módulos do Linux para encontrar suas vulnerabilidades.
- DDoS

1. KrebsOnSecurity.com: O blog do pesquisador Brain Krebs sofreu um ataque DDoS de 623 Gbps em 30 de setembro de 2016, o ataque ocorreu através de um grande número de dispositivos IoT comprometidos (KREBS, 2016b). Este ataque DDoS foi considerado como uma retaliação contra os diversos artigos de Krebs sobre a retirada do provedor israelense chamado vDOS, que coincidiu com as prisões de dois homens (KREBS, 2016a).

O ataque foi lançado por cerca de 24.000 dispositivos IoT, principalmente câmeras IP e gravadores de vídeo (DVR) rodeados pelo mundo que estavam infectados com Mirai ou BASHLITE malware (KREBS, 2016b). O tráfego de ataque consistia principalmente em tráfego de lixo eletrônico, como inundações SYN, GET e POST.

2. OVH: Em 22 de setembro de 2016, Octave Klaba fundador da empresa OVH que oferece servidores dedicados, privados e outros serviços da web, publicou em sua rede social que os servidores da OVH estavam recebendo uma série de ataques DDoS e muitos deles maiores que 100 Gbps, o maior ataque documentado pela OVH chegou a 799 Gbps (MILLMAN, 2016).

Em 23 de setembro de 2016, Klaba postou novamente em sua rede social que a OVH recebeu uma série de ataques por 145.606 dispositivos IoT como câmeras e DVR supostamente infectados com o Mirai e BASHLITE, sendo que cada dispositivo enviou entre 1 e 30 Mbps gerando cerca de 1,1 Tbps a 1,5 Tbps de tráfego principalmente do tipo TCP Ack, TCP Ack + PSH e TCP SYN (MILLMAN, 2016).

O ataque de OVH foi o maior ataque lançado até hoje.

3. DYN: Dyn é uma empresa que oferece uma ampla variedade de produtos para controlar e otimizar a infraestrutura online, além de ser uma das líderes de provedor DNS do mundo. Em 21 de outubro de 2016, a Dyn recebeu um ataque DDoS por cerca de 100.000 dispositivos IoT, a maioria infectados pela rede Mirai, alcançando cerca de 1,2 Tbps, com o tráfego TCP e UDP mascarados na porta 53 (HILTON, 2016). Dyn fornece seu serviço de gerenciamento de DNS para sites famosos como Amazon, Spotify, Airbnb, GitHub, HBO, Netflix, PayPal, Twitter e muitos outros que ficaram completamente ou parcialmente indisponíveis para seus usuários na Europa e América do Norte.
4. Bancos Russos: Oito diferentes bancos russos sofreram ataques DDoS em outubro de 2015 e entre 8 de novembro a 10 de novembro de 2016 mais cinco bancos russos sofreram ataques prolongados a partir de 24.000 dispositivos IoT distribuídos em torno de 30 países (CUTHBERTSON, 2016).
5. WikiLeaks: Em 7 de novembro de 2016 os servidores da WikiLeaks sofreram ataques que duraram quase 24 horas, o ataque foi em resposta ao “DNSLeak2”,

usado para restringir a liberdade de expressão na Internet. O Google iniciou o Project Shield para fornecer serviços contra ataques de negação de serviços gratuitamente para sites que possuem conteúdos relacionados aos direitos humanos, o site krebsonsecurit.com é um dos sites que utiliza esse projeto para se manter mais seguro (UZUNOVIC, 2016).

6. Eleições dos EUA: A empresa de segurança da Internet Flashpoint relatou ataques DDoS do botnet Mirai nos sites da campanha de Donald Trump e da Hillary Clinton, no entanto não houve uma interrupção dos serviços (NIXON, 2016).

4.3 Melhores práticas de segurança em câmeras IP

Não é fácil minimizar as brechas de um sistema de monitoramento por câmeras IP, para reduzir as vulnerabilidades presentes em um sistema de vídeo-monitoramento é extremamente necessária uma postura preventiva por parte dos fabricantes, instaladores e usuários, além disso, é importante ter a consciência de como ocorre as invasões para proteger melhor o sistema de vigilância. Não existe um produto totalmente seguro, mas os usuários e os fabricantes devem tomar medidas que minimizem as vulnerabilidades dos dispositivos conectados à rede.

Senhas fortes: ao instalar câmeras de segurança nas residências ou empresas, é importantíssimo alterar a senha padrão do dispositivo para uma senha grande e complexa, uma senha forte consiste em uma sequência de números, letras e caracteres especiais. Essa preocupação com a senha minimiza consideravelmente as chances de que outras pessoas realizem o acesso indevido nas câmeras, simplesmente por adquirir o usuário e a senha padrão ao acessar o manual do dispositivo disponível na Internet, ou por meio de ataque de força bruta e ataque de dicionário.

Uma sugestão para senhas mais seguras, seria criar senhas com no mínimo 8 caracteres, combinando letras maiúsculas, minúsculas, números e símbolos, evitando datas de aniversário, senhas sequenciais e senhas com palavras do dicionário.

Por exemplo, para criarmos uma senha forte e de fácil lembrança podemos memorizar uma frase para ser a base da senha: “Eu sou capaz vou ser aprovado no TCC e ganharei muito dinheiro”, gerando EscvsanTegm\$, com as iniciais da frase e no final o símbolo do dinheiro.

Para evitar ataques onde o hacker explora os serviços do dispositivo a fim de encontrar vulnerabilidades para um posterior ataque, é importante realizar uma manutenção periódica nos dispositivos, sempre atualizando seu *firmware*.

A grande maioria dos dispositivos estão vulneráveis pelo fato do cliente não querer

pagar por uma manutenção periódica, essa atitude de querer economizar com gastos necessários, faz com que o cliente sofra invasões e nem mesmo sabem sobre essas invasões, já que o invasor pode aproveitar das brechas, invadir o sistema e apagar todos os logs de evidências que esteve logado no dispositivo.

É possível que o próprio cliente atualize o *firmware* de suas câmeras, para isso é necessário verificar frequentemente o site do fabricante da câmera IP se há atualizações de *firmwares*.

Há também a questão dos fabricantes, especialmente as marcas mais baratas, não darem muita atenção para atualizações de *firmware*, por isso é importante também pesquisar e escolher os produtos de fabricantes mais conhecidos, que lançam constantemente atualizações do *firmware* de seus produtos.

É importante que aquelas pessoas que possuem senhas ou acesso direto aos sistemas se preocupem com a segurança, pois ela pode ser uma vulnerabilidade física para o invasor, o invasor pode encontrar senhas anotadas, ter acesso a equipamentos logados ou realizar a engenharia social, que se trata de uma manipulação psicológica onde o invasor utiliza a persuasão para obter informações confidenciais.

Se a câmera IP estiver com conexão *wireless*, é de fundamental importância a conexão em uma rede sem fio WPA2, para que essa criptografia evite que invasores consigam conectar-se ao dispositivo e acessar às imagens.

Uma forma de evitar um ataque chamado man-in-the-middle, onde o atacante intercepta a senha enviada do cliente para o servidor, é utilizando uma criptografia da senha enviada e também através de uma conexão segura via *Virtual Private Network* (VPN).

A questão de segurança da Internet das coisas levou as empresas líderes em tecnologia a se preocuparem com as consequências que podem ocorrer quando violado a segurança dos dispositivos, preocupações até no nível do governo federal. Então foi fundada o iotsecurityfoundation.org, um órgão sem fins lucrativos que verifica vulnerabilidades e falhas em dispositivos conectados à Internet e oferece assistência de segurança a provedores de tecnologia, fabricantes de dispositivos e usuários finais (DICKSON, 2015).

4.3.0.1 Recomendações para os usuários

- Conscientizar-se e estudar as áreas de rede e segurança da informação.
- Analisar os riscos de ameaças potenciais e seus possíveis danos, caso o sistema seja invadido.
- Usar câmeras de fabricantes conhecidos, que tenham suporte técnico e que frequentemente disponibilizam atualizações de *firmware*.

- Eventualmente trocar a senha de acesso da sua câmera de segurança IP, e nunca deixar a senha padrão do fabricante, recomendável a utilização de senhas fortes e individuais.
- Trocar as portas padrões de acesso à câmera IP.
- Desabilite recursos que não estão sendo usados, como por exemplo FTP, DDNS, P2P, ONVIF e SMTP.
- Proteger a câmera IP com firewalls.
- Utilizar criptografia entre as câmeras e os dispositivos remotos, mesmo em redes locais.
- Utilizar recursos de segurança de rede como protocolos de segurança e VPNs. Separar a rede de acesso das câmeras com a rede de dados.
- Evitar o uso de DMZ para ter acesso remoto ao dispositivo.
- Configurar o RTSP Permission Check, solicitando autenticação para acessar o dispositivo.
- Desativar a (Plug e Play Universais) UPnP em seus roteadores para impedir a abertura de entradas de Internet externas sem qualquer aviso de dispositivos dentro da rede.
- Verificar regularmente o registro de acessos, para detectar acessos não autorizados.
- Investigar o histórico de segurança do fabricante para compreender as funcionalidades dos dispositivos, a fim de elaborar um modelo de riscos e ameaças e verificar se o dispositivo pode ser corrigido caso necessário.
- Empresas podem comprar serviços de proteção anti-DDoS oferecidos por ISPs e CDNs como Akamai, Dyn e outros.

4.3.0.2 Recomendações para os fabricantes

De acordo com a F-secure, os fabricantes são responsáveis por garantir a segurança dos dispositivos em última instância, e para isso os fabricantes devem tomar algumas ações como:

- Exigir que os usuários alterem a senha padrão no ato da instalação do dispositivo.
- Bloquear conta de configuração após falha em tentativas de login, para evitar ataques de força bruta.

- Sempre citar entrada que acaba com comandos executados pelo shell, ou usar funções de família exec. Evite chamadas do sistema. Impossibilite a chamada do execl com "sh -c s", pois isso é igual a uma chamada do sistema.
- Evite scripts de shell não confiável na inicialização.
- Remova o processamento de entrada inseguro (sprintf, strcpy, strcat, memcpy com comprimento não confiável etc).
- Use uma senha administrativa padrão verdadeiramente aleatória e adicione um adesivo na parte inferior do dispositivo com a senha.
- Desativar o usuário do arquivo passwd.
- Remova a funcionalidade oculta desnecessária, como ser capaz de habilitar o telnetd.
- Remova as credenciais embutidas da fábrica.
- Implementar o firewall apropriado do iptables.
- Corrigir permissões de arquivo e diretórios graváveis.
- Execute sempre a codificação adequada de caracteres especiais HTML.
- Proibir o ONVIF anônimo.
- Conscientizar-se e certificar seus dispositivos em órgão regulamentadores, promovendo a segurança por parte do fabricante e das autoridades nacionais.

5 Desenvolvimento prático

Neste capítulo será abordado todo o ambiente prático realizado, a fim de descrever a importância de implementar todos os métodos de segurança recomendadas no capítulo anterior, além de considerações sobre os testes de segurança realizadas em um ambiente seguro, conforme caracterizado pelo software iVMS-4200 na figura abaixo.

Tipo de Equip	Alcunha	Modo de Li...	Parâmetros de rede	N.º de série do dispositivo	Segurança	Estado da rede	Atualização de f...	Atualizar
Dispositivo ...	tccaugusto	TCP/IP	192.158.1.11:8000	D5-2CD1101-120170821AAWR318322374	Forte		Não atualizável	

Figura 18 – Nível de segurança.

Fonte: Elaborada pelo autor

A seguir segue uma descrição dos dispositivos, protocolos, software e métodos utilizados para o desenvolvimento do caso de uso.

5.1 Dispositivos

Para uma melhor compreensão dos dispositivos utilizados, a figura 19 representa uma visão geral do sistema de monitoramento utilizado para os testes.

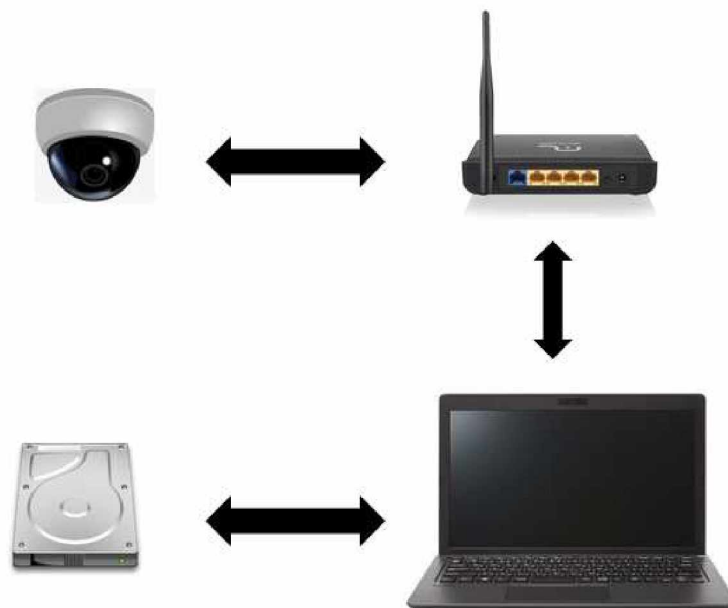


Figura 19 – Diagrama representativo do sistema desenvolvido

Fonte: Elaborada pelo autor

Foi utilizado o roteador VR-3031u 802.11 Multi-DSL que suporta ADSL2+ e VDSL2, o VDSL2 é uma tecnologia triple play (vídeo, voz e dados). O dispositivo vem com portas 10/100 Base-T Ethernet e uma USB Host, combinando conectividade de LAN com fio e um 802.11 n WiFi Ponto de acesso WLAN integrado (AP) para conectividade sem fio.

O Aparelho foi utilizado para conectar a câmera sem fio, a central e a um computador ou celular pessoal. Caso haja necessidades de um alcance maior do sinal wireless ou uma taxa de transferência maior, o roteador pode ser substituído por um mais potente.

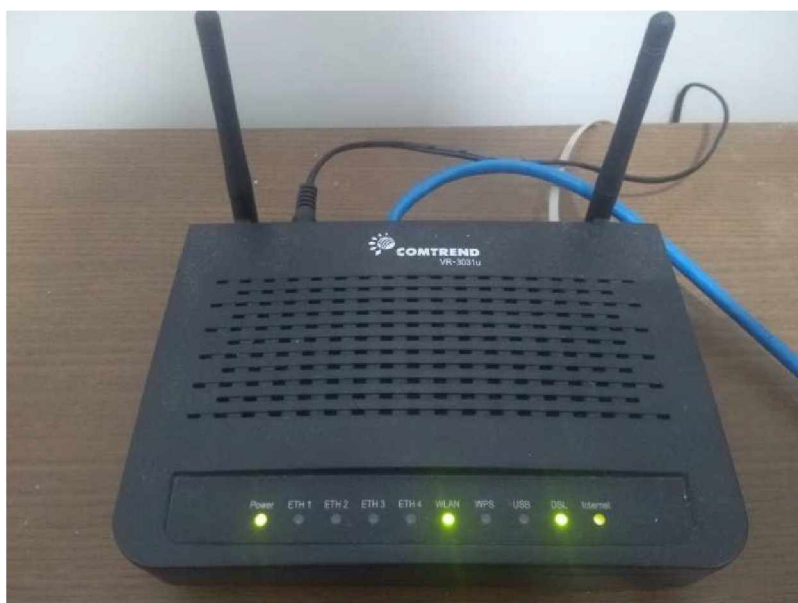


Figura 20 – Roteador utilizado para conectar as câmeras, a central e o computador pessoal do usuário.

Fonte: Elaborada pelo autor

A câmera usada foi a câmera dome IP modelo DS-2CD1101-I da Hikvision é indicada para instalação em ambientes internos. Possui resolução de 1Mp, lente de 2.8mm, infravermelho com capacidade de atingir 30 m e as certificações IP67, IK10, ou seja, resistente a água, poeira e vandalismo. Todas estas características permitem gerar filmagens diurnas e noturnas em alta qualidade.

A câmera possui proteção por usuário e senha, detecção de movimento com notificação no Software Cliente, acesso remoto via Browser Internet Explorer e Software Cliente, além de suportar os protocolos Onvif, PSIA, CGI, TCP/IP, HTTP, DHCP, DNS, PPPoE, RTP / RTCP.

O Ultrabook utilizado foi um ASUS S46C, com processador Intel core i7 3517U terceira geração, memória ram de 6 GB e HD de 750 GB, além de uma memória não volátil utilizada para salvar as imagens capturadas pela câmera, conforme figura 22.



Figura 21 Câmera utilizada para realizar a aquisição das imagens de vigilância.

Fonte: Elaborada pelo autor

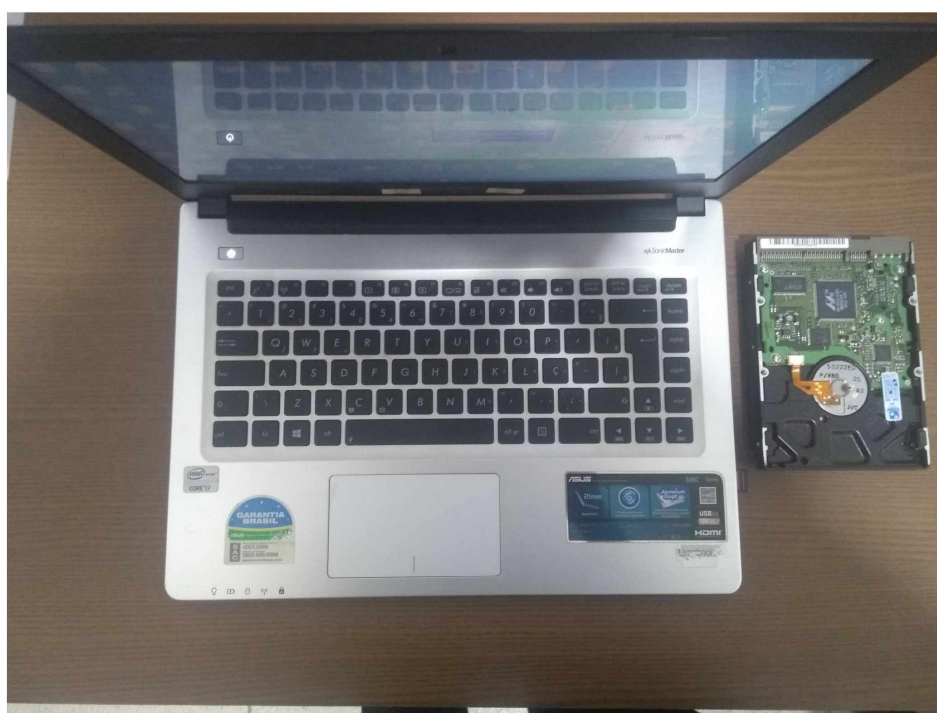


Figura 22 – Computador e memória não volátil utilizados.

Fonte: Elaborada pelo autor

5.2 Protocolos de comunicação

Na camada de Aplicação, o protocolo File Transfer Protocol (FTP) é utilizado para a transferência e armazenamento das imagens. Além do FTP, existe o Hypertext Transfer Protocol (HTTP) utilizado para configurar o sistema através de uma página web

disponibilizada pela própria fabricante Hikivision.

Na camada de Transporte, foi utilizado o protocolo TCP para realizar a comunicação entre a câmera e a central, foi utilizado o TCP ao invés do UDP pelo fato de que o TCP oferece mais segurança na transmissão dos dados.

Na camada de Rede, foi utilizado o protocolo Internet Protocol version 4 (IPv4) para o encaminhamento de pacotes de dados pela rede, tanto para a central como para a câmera.

Já na camada de Acesso, foi utilizado os protocolos Ethernet 802.3 e 802.11 com conexões feitas via cabo de rede e sem fio respectivamente.

Camadas do modelo TCP/IP	
Aplicação	HTTP e FTP
Transporte	TCP
Rede	IPv4
Acesso	Ethernet 802.3 e 802.11 (wireless)

Figura 23 – Figura protocolos de comunicação – Camadas do modelo TCP/IP e seus respectivos protocolos utilizados.

Fonte: Elaborada pelo autor

5.3 Software

O software para gerenciamento de vídeo utilizado foi o iVMS-4200 da própria fabricante, ele pode ser usado para DVRs, NVRs, câmeras IP e codificadores, fornecendo várias funcionalidades como gravação e visualização das imagens ao vivo, pesquisas e reprodução remota, programar ações como enviar um e-mail ou sms e acionar um alarme em situações programada com a detecção de movimento, além da função de melhorar a segurança criptografando as informações confidenciais do banco de dados.

O Nmap é um software livre utilizada para descobrir serviços em um sistema conectado à internet, essa ferramenta permite varreduras de portas TCP e UDP abertas, detecção de sistema operacionais e versões dos componentes da rede e interação de scripts para procurar falhas de segurança. No ambiente de teste foi utilizado o Zenmap, que consiste em um aplicativo multiplataforma (Windows, Linux, Mac OS X, etc.) escolhido

por corresponder uma versão do Nmap com interface, tornando mais prático e fácil seu uso.

5.4 Considerações sobre o desenvolvimento

No ambiente prático desenvolvido, ocorreram poucos problemas inesperados e complicações. Após a instalação e configuração da câmera, as imagens captadas não eram transmitidas pelo navegador Web por causa de uma falha de plugin do próprio fabricante, onde a alternativa foi desinstalar o plugin e gerenciar as imagens capturadas pelo próprio software iVMS-4200 visto que o mesmo oferece mais praticidade e segurança, nas figuras 21 e 22 refere-se à qualidade da imagem obtida pela câmera em um ambiente com e sem luz.

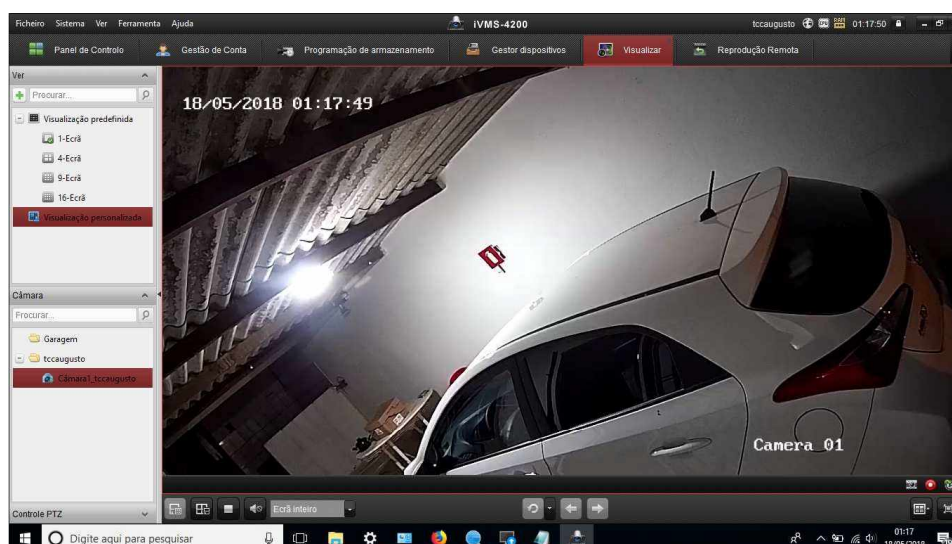


Figura 24 – Imagem capturada em um ambiente com luz.

Fonte: Elaborada pelo autor

Em se tratando de medidas adotadas para aumentar a segurança do sistema de monitoramento, foi executado todas as ações mencionadas no capítulo anterior, o que comprova a importância de uma política de segurança para minimizar as vulnerabilidades e tornar o ambiente desenvolvido mais seguro, haja visto que foram realizadas tentativas de ataques sem sucesso.

Algumas ações merecem considerações mais detalhadas para que o projeto possa ser melhor compreendido, conforme é apresentado a seguir.

Primeiramente foram realizados testes com um software que foi desenvolvido para explorar uma vulnerabilidade das câmeras IP fabricadas pela Hikvision, seu nome é Hikvision Password Reset que permite acessar a câmera sem necessitar saber o usuário e a



Figura 25 – Imagem capturada em um ambiente sem luz.

Fonte: Elaborada pelo autor

senha, apenas com o endereço IP e a porta da câmera podemos facilmente ter acesso como administrador.

Sabendo o endereço IP e a porta do dispositivo, é possível buscar quais são os usuários configurados para o dispositivo e com o usuário, conseguimos redefinir sua senha, permitindo o acesso de administrador fácil e rápido, conforme ilustrado na figura 26.

Esse ataque não foi bem-sucedido no ambiente de teste, haja visto que o firmware do dispositivo estava atualizado, com todas as falhas já reportadas ao fabricante corrigidas, o que impossibilitou a execução desse acesso direto.

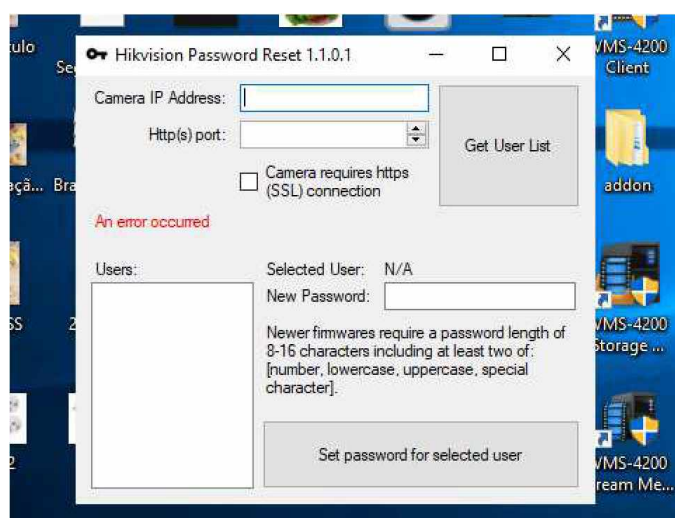


Figura 26 – Hikvision Password Reset.

Fonte: Elaborada pelo autor

Outro teste realizado foi simulando um ataque de força bruta, onde após consecutivas falhas de login, o próprio sistema da Hikvision bloqueou a conta de configuração por um período de 30 minutos, tanto para o acesso pelo navegador, quanto pelo iVMS-4200, conforme ilustrado na figura 27.

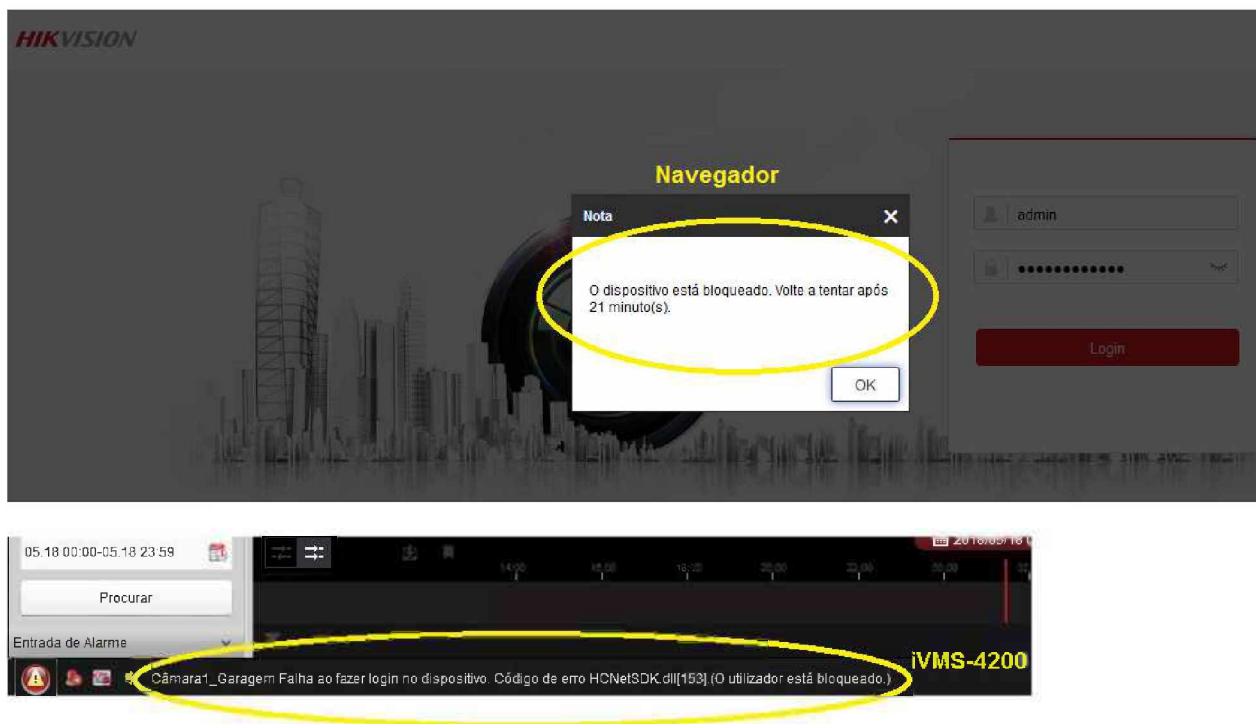


Figura 27 – Bloqueio de conta após falhas de login.

Fonte: Elaborada pelo autor

Por padrão a câmera possui vários recursos que já vem habilitados de fábrica, como por exemplo o RTSP, FTP, DDNS, SMTP e acesso remoto. No capítulo anterior recomenda-se que seja desabilitado todos os recursos que não estão em uso. O RTSP é um recurso em uso, que serve para acessar a câmera pelo celular ou pelo software do PC, ele já vem habilitado e utiliza por padrão a porta 554, mas possui uma vulnerabilidade nesse recurso que também foi facilmente resolvida. Nas configurações do dispositivo possui uma opção chamada “Activar Bloqueio de Registo Irregular” que não estava ativado, o que permite uma comunicação RTSP sem autenticação, sendo necessário apenas utilizar o script “rtsp-url-brute” para realizar o scanner no NMAP e encontrar as URL’s do RTSP, com posse da URL e com o auxílio de um software para streaming de vídeo como o QuickPlay, ocorreu o acesso a streaming da câmera conforme ilustrado na figura 28.

Para evitar essa vulnerabilidade foi necessário apenas ativar o “Activar Bloqueio de Registo Irregular”, para sempre exigir uma autenticação com usuário e senha toda vez que for realizar uma comunicação RTSP, conforme indicado na figura 29.

Diversos outros scripts foram executados pelo nmap, para testar as vulnerabilida-

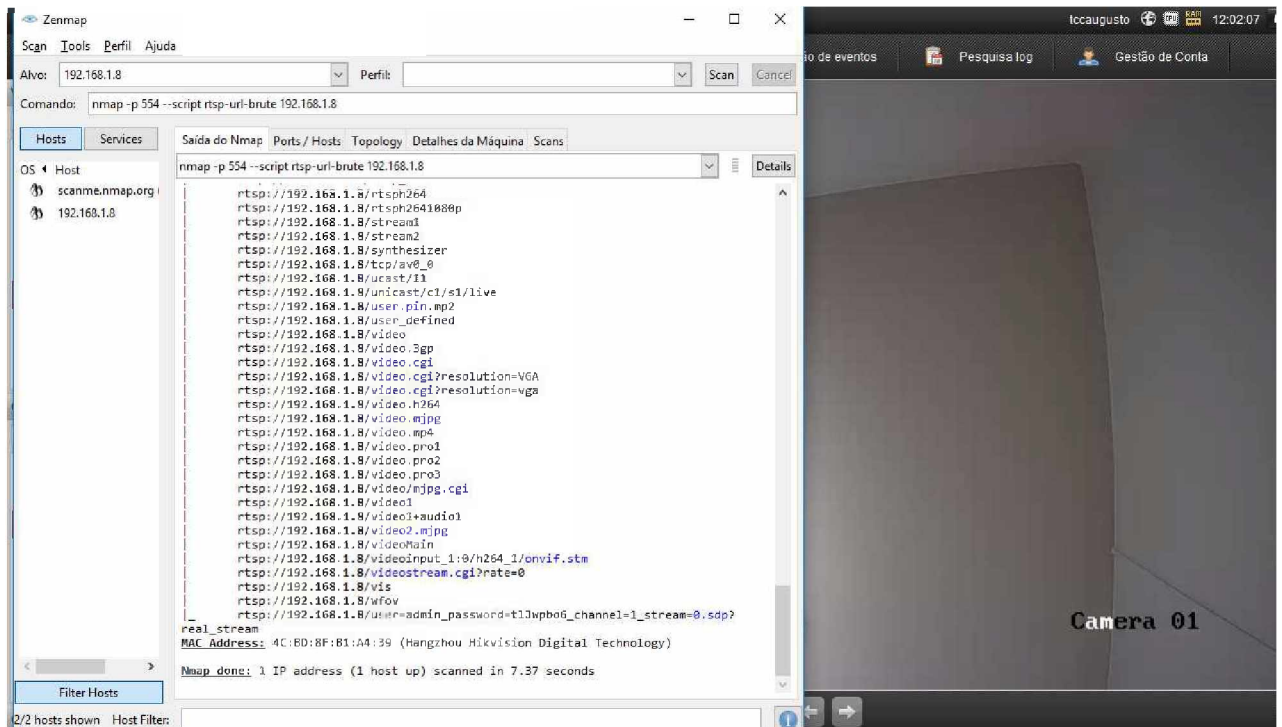


Figura 28 – scanner com NMAP utilizando o script rtsp-url-brute para encontrar as URL's do RTSP.

Fonte: Elaborada pelo autor

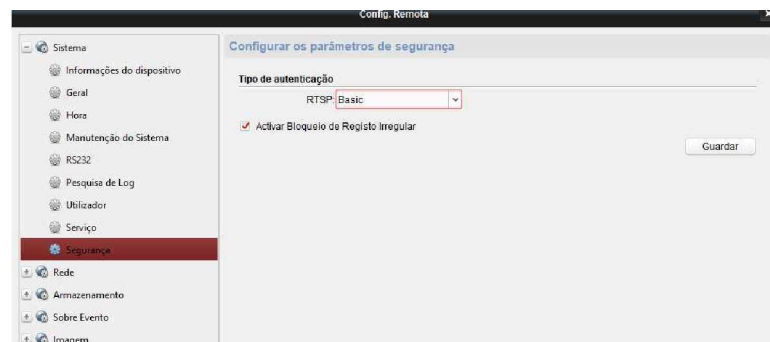


Figura 29 – Ativando o bloqueio de registro irregular.

Fonte: Elaborada pelo autor

des da câmera, porém não foi encontrado nenhuma outra brecha no ambiente de teste, o que confirma o nível de segurança caracterizado pelo software iVMS-4200, ilustrado na figura 18.

5.5 Avaliação do fabricante

Com base nos testes e estudos realizados, conclui-se que o fabricante Hikvision se consolidou no mercado devido aos seus produtos de qualidade, seu suporte ao cliente e

toda sua preocupação com a segurança de seus produtos.

No site da empresa encontramos todos os arquivos para downloads necessários para configuração e instalação de seus dispositivos, como softwares, firmware e manuais, além de registros das falhas reportadas para a fabricante com suas correções.

É de grande valia ressaltar a facilidade e segurança para instalar e configurar a Camera IP utilizada neste projeto, vários aspectos primordiais constatados no teste estão relatado a seguir.

Primeiramente já é solicitado a criação de uma senha, impossibilitando ataques por credenciais padrão.

Após falhas em tentativas de login, o sistema bloqueou a conta de configuração por 30 minutos tanto para o acesso pelo navegador, quanto pelo iVMS-4200, o que evita o ataque de força bruta, conforme ilustrado na figura 27.

Disponibilização de atualizações de firmware fácil e rápida no próprio IVMS-4200 ou na página de configuração acessada pelo navegador web. Fácil configuração e instalação de firewall.

Certificação dos dispositivos em órgão regulamentadores.

6 Conclusão

Este trabalho teve como objetivo demonstrar de maneira concisa, soluções de segurança para minimizar as vulnerabilidades presentes nas câmeras IP.

A implementação deste projeto envolveu os principais conceitos teóricos de redes, segurança da informação e das câmeras IP, o que possibilitou uma visão clara das melhores práticas para minimizar essas ameaças. No capítulo 5, foi realizado um estudo prático para testar as vulnerabilidades relatadas e as soluções propostas.

É evidente que não existe um sistema de vídeo-monitoramento por câmeras IP 100% seguro, porém existem diversas formas de diminuir os riscos, desde ações mais simples como o uso de senhas seguras, uso de equipamentos mais seguros e confiáveis, constantes atualizações do firmware, manutenções periódicas como ações mais complexas como a contratação de uma proteção contra ataques.

A segurança das câmeras IP não depende apenas dos seus usuários, mas também dos fabricantes, que devem garantir que seus dispositivos permaneçam seguros e sempre atualizados, garantindo a redução de vulnerabilidades e riscos de ataques pela Internet. Muitos desses fabricantes ignoram o fornecimento de atualizações de firmware para seus usuários, o que deixa a maioria dos dispositivos vulneráveis.

Sendo assim, é de grande importância que o processo de configuração tanto da rede quanto dos dispositivos tenha certos cuidados, sendo fundamental um acompanhamento adequado e constante na manutenção dos dispositivos, para que se possa perceber quaisquer modificações, evitando futuras consequências.

Logo, fica claro a necessidade de uma política de segurança sólida, que não se restrinja apenas nas ameaças conhecidas e que sejam periodicamente atualizadas, bem como basear essa política de segurança em camadas, visto que os atacantes não exploram apenas uma técnica de invasão, mas um conjunto delas, comprometendo a segurança de todo o sistema de monitoramento.

Nesse sentido, mesmo que os objetivos iniciais tenham sido cumpridos, é fato que os CFTVs tenham muito a amadurecer, como sugestão de trabalhos futuros, pode-se realizar novos estudos de vulnerabilidades não conhecidas, além de uma análise completa das ameaças presentes em todos os componentes de um CFTV, como: DVR, NVR e roteadores, visto que estes dispositivos podem comprometer a segurança de todo o sistema de monitoramento.

Referências

- BEZERRA, F. F. *Ferramenta de Análise Modal De Protocolos de Segurança para Redes Sem Fio*. 2014. Monografia apresentada como conclusão do curso De Engenheiro de telecomunicações, Universidade Regional de Blumenau. Citado na página 9.
- BÄCHER P., H. T. K. M.; WICHERSKI. Know your enemy: Tracking botnets. *The Honeynet Project e Research Alliance*, 2007. Disponível em: <<http://www.honeynet.org/papers/bots/>>. Acesso em: 19 jun. 2017. Citado na página 10.
- CERT. *Cartilha de Segurança para Internet*. [S.l.], 2012. Disponível em: <<http://cartilha.cert.br/malware>>. Acesso em: 30 jun. 2017. Citado 3 vezes nas páginas 10, 25 e 26.
- CLULEY, G. Hacked shopping mall cctv cameras are launching ddos attacks. *Tripwire*, 2015. Disponível em: <<https://www.tripwire.com/state-of-security/securitydata-protection/hacked-shopping-mall-cctv-cameras-are-launching-ddos-attacks/>>. Acesso em: 09 jun. 2017. Citado na página 10.
- CUTHBERTSON, A. Russian banks become latest victim of mirai cyberattacks. 2016. Disponível em: <http://www.theregister.co.uk/2016/11/11/russian_banks_ddos/>. Acesso em: 20 mar. 2018. Citado na página 44.
- DICKSON, B. Why iot security is so critical. 2015. Disponível em: <<https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical>>. Acesso em: 30 Dez. 2017. Citado na página 46.
- DUCKLIN, P. Deutsche telkom outage mirai botnet goes double rogue. *Naked Security*, 2016. Disponível em: <<https://nakedsecurity.sophos.com/pt/2016/11/29/deutsche-telkom-outage-mirai-botnetgoes-double-rogue>>. Acesso em: 30 jun. 2017. Citado 2 vezes nas páginas 10 e 39.
- HENRIQUE, R. F-secure publica estudo sobre falhas em câmeras da foscam. 2017. Disponível em: <<http://www.abctec.com.br/f-secure-publica-estudo-sobre-falhas-em-cameras-da-foscam/>>. Acesso em: 19 sep. 2017. Citado na página 43.
- HILTON, S. Dyn analysis summary of friday october 21 attack. 2016. Disponível em: <<https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>>. Acesso em: 20 mar. 2018. Citado na página 44.
- KREBS, B. 10 alleged vdos proprietors arrested in israel. *Naked Security*, 2016. Disponível em: <<https://krebsonsecurity.com/2016/09/alleged-vdos-proprietors-arrested-in-israel/>>. Acesso em: 20 feb. 2018. Citado na página 44.
- KREBS, B. Câmeras hackeadas, dvrs alimentaram a interrupção maciça da internet de hoje. *Naked Security*, 2016. Disponível em: <<https://krebsonsecurity.com/2016/10/hackedcameras-dvrs-powered-todays-massive-internet-outage>>. Acesso em: 30 jun. 2017. Citado 3 vezes nas páginas 10, 40 e 44.

KUROSE, J. F. *Redes de computadores e a internet*. 5. ed. São Paulo: Pearson, 2010. Citado 3 vezes nas páginas 12, 13 e 14.

MICHAEL, M. F-secure vulnerabilities in foscam ip cameras report. 2017. Disponível em: <<https://press.f-secure.com/2017/06/07/vulnerabilitiesfoscamipcamerareport>>. Acesso em: 19 sep. 2017. Citado 2 vezes nas páginas 40 e 42.

MILLMAN, R. Ovh suffers 1.1 tbps ddos attack. 2016. Disponível em: <<https://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/532197/>>. Acesso em: 20 mar. 2018. Citado na página 44.

NBR ISO/IEC 27002:2005 – Tecnologia da informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. Citado 3 vezes nas páginas 21, 22 e 23.

NIXON, A. flashpoint monitoring of mirai shows attempted ddos of trump and clinton websites. 2016. Disponível em: <<https://www.flashpoint-intel.com/blog/trending/attempted-ddos-trump-and-clinton-websites/>>. Acesso em: 20 mar. 2018. Citado na página 45.

RUFINO, N. M. d. O. *Segurança em redes sem fio*. 2. ed. São Paulo: Novatec, 2005. Citado 3 vezes nas páginas 10, 18 e 29.

TANENBAUM, A. S. *Computer networks*. 5. ed. São Paulo: Pearson, 2011. Citado 2 vezes nas páginas 15 e 16.

TECNOLOGIA de vídeo em rede. [S.l.], 2013. Disponível em: <<https://www.axis.com/br/pt/learning/web-articles/technical-guide-to-network-video>>. Acesso em: 17 nov. 2017. Citado 4 vezes nas páginas 32, 33, 37 e 38.

THE DDoS that didn't break the camel's VAC. 2016. Disponível em: <<https://www.ovh.com/world/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac>>. Acesso em: 30 Dez. 2017. Citado na página 40.

UZUNOVIC, A. Wikileaks releases dncleak2; suffers massive ddos attack. 2016. Disponível em: <<https://www.hackread.com/wikileaks-dncleak2-suffers-massive-ddos-attack/>>. Acesso em: 20 mar. 2018. Citado na página 45.