UMA ABORDAGEM DE SEGURANÇA UTILIZANDO O PROTOCOLO SIP EM DISPOSITIVOS EMBARCADOS

ISBN: 978-85-9591-077-5

"ANONYMOUS HACKER"
DESIGNED BY FREEPIK

Toniclay Andrade Nogueira
Adauto Cavalcante Menezes
José dos Santos Machado
Admilson de Ribamar Lima Ribeiro
Edward David Moreno Ordonez

INSTITUTO FEDERAL
Sergipe

Toniclay Andrade Nogueira
Adauto Cavalcante Menezes
José dos Santos Machado
Admilson de Ribamar Lima Ribeiro
Edward David Moreno Ordonez

Uma abordagem de segurança utilizando o protocolo SIP em dispositivos embarcados

INSTITUTO FEDERAL
Sergipe

Copyright © 2018 • IFS

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida em nenhuma forma e por nenhum meio mecânico, incluindo fotocópia, gravação ou qualquer sistema de armazenamento de informação, sem autorização expressa dos autores ou do IFS.

EDITORA-CHEFE
Vanina Cardoso Viana Andrade

CONSELHO EDITORIAL
Diego Ramos Feitosa
Jéssika Lima Santos
Júlio César Nunes Ramiro
César de Oliveira Santos
Kelly Cristina Barbosa
Salim Silva Souza

PLANEJAMENTO E COORDENAÇÃO GRÁFICA
Jéssika Lima Santos

PROJETO GRÁFICO DA CAPA
André Azevedo

DIAGRAMAÇÃO
Jéssika Lima Santos
Laryssa Mota Santos Silva

REVISÃO
Toniclay Andrade Nogueira

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

A154 Uma Abordagem de Segurança Utilizando o Protocolo SIP em dispositivos embarcados. [recurso eletrônico] / Toniclay Andrade Nogueira ... [et al]. – Aracaju: IFS, 2018.
74 p. : il.

Formato: e-book
ISBN: 978-85-9591-077-5

1. Dispositivos embarcados. 2. Protocolo SIP - Segurança. 3. Redes de computadores 4. Tecnologia VoIP 5. Telecomunicação – Redes de computadores I. Nogueira, Toniclay Andrade. II. Menezes, Adauto Cavalcante. III. Machado, José dos Santos. IV. Ribeiro, Admilson de Ribamar Lima. V. Ordonez, Edward David Moreno. VI. Título.

CDU: 004.057.4

Ficha catalográfica elaborada pela bibliotecária Célia Aparecida Santos de Araújo CRB 5/1030

[2018]
Instituto Federal de Educação, Ciência e Tecnologia de Sergipe (IFS)
Avenida Jorge Amado, 1551. Loteamento Garcia, Bairro Jardins
Aracaju/SE. CEP: 49025-330
TEL.: +55 (79) 3711-3222 E-mail: edifs@ifs.edu.br
Impresso no Brasil

MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE (IFS)

PRESIDENTE DA REPÚBLICA
Jair Messias Bolsonaro

MINISTRO DA EDUCAÇÃO
Ricardo Vélez Rodríguez

SECRETÁRIA DA EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
Alexandro Ferreira de Souza

REITORA DO IFS
Ruth Sales Gama de Andrade

PRÓ-REITORA DE PESQUISA E EXTENSÃO
Chirlaine Cristine Gonçalves

Dedico esta obra aos técnicos e analistas da área de tecnologia da informação que desejam realizar rigorosos testes de segurança em protocolo SIP com Dispositivo embarcados.

Lista de ilustrações

Figura 1 – Projeto de cenário teste 21
Figura 2 – Cenário do funcionamento ideal da aplicação VoIP 24
Figura 3 – Diagrama básico de um sistema embarcado dotado de um micro controlador monitorando o ambiente 27
Figura 4 – Raspberry Pi 3 29
Figura 5 – Visão geral do SIP 32
Figura 6 – Ataque de negação de serviço em servidor SIP 34
Figura 7 – SIP Signalling Loop 35
Figura 8 – Assistente de Máquina Virtual 38
Figura 9 – *Software* Zabbix 39
Figura 10 – Cenário real de testes 45
Figura 11 – Raspberry Pi 3 e o circuito INA219 medidor de energia 46
Figura 12 – Varredura de rede através do comando smvmap 47
Figura 13 – Resultado da Varredura de rede através do comando smvmap 47
Figura 14 – O atacante identifica uma extensão, a extensão 100 48
Figura 15 – Mensagem SIP trocada 49
Figura 16 – Resposta com informações do registro 50
Figura 17 – Envio de pacote de REGISTER 51
Figura 18 – Ativação do arpspoof 54
Figura 19 – Captura de pacotes com wireshark 55
Figura 20 – Estado do Raspberry Pi 3 antes do ataque 56
Figura 21 – comando inviteflood 57
Figura 22 – Resultado do ataque de DoS 58
Figura 23 – Uso da Memória e CPU 59

Figura 24 – Cenário para coleta de eficiência do Processador e Memória **60**

Figura 25 – Eficiência da Memoria **61**

Figura 26 – Eficiência do Processador **61**

Figura 27 – consumo de Memoria e CPU em Ataque DoS **62**

Figura 28 – 4.000.000 pacotes em CPU em Ataque DoS **63**

Figura 29 – Dispositivo embarcado Arduino Uno com Raspberry Pi 3 com Asterisk **64**

Figura 30 – coleta de eficiência energética inicial x coleta de eficiência energética Ataque de Autenticação e no Ataque Man-in-the-middle **65**

Figura 31 – Eficiência energética no Ataque de Negação de Serviço - DoS **67**

Lista de tabelas

Tabela 1 – Comparação entre os trabalhos correlatos 43
Tabela 2 – *Softwares* utilizados no experimento 45
Tabela 3 – Análise de Ataque DoS por quantidade de pacotes 58
Tabela 4 – Coleta da eficiência energética inicial. 64
Tabela 5 – Coleta de eficiência energética nos Ataque de Autenticação e no Ataque Man-in-themiddle 65
Tabela 6 – Coleta da eficiência energética no Ataque de Negação de Serviço - DoS 66

Lista de abreviaturas e siglas

APIs	Application Programming Interface
Arp	Address Resolution Protocol
CADC	Air Data Central Computer
DNS	Domain Name System
DoS	Denial Of Service
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
PABX	Private Automatic Branch Exchange
PSTN	Public Switched Telephone Network
PBX	Private Branch Exchange
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman
RTP	Real Time Protocol
SIP	Session Initiation Protocol
SIPp	Self Invested Personal Pension
Snort	É um software livre de detecção de intrusão para rede
SQL	Structured Query Language

TCP	Protocolo de Controle de Transmissão
TLS	Transport Layer Security
UAC	User Agent Client
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

Sumário

1 Introdução 17

1.1 Problemática e Hipótese 19
1.2 Objetivos 19
1.3 Justificativa 20
1.4 Metodologia 20
1.5 Organização do livro 22

2 Fundamentação Teórica 23

2.1 VoIP 23
2.2 Sistemas Embarcados 26
2.3 Raspberry Pi 3 28
2.4 Asterisk 29
2.5 Protocolo *Session Initiation Protocol* (SIP) 31
2.5.1 Tipos de ataques aos Protocolos SIP 32
2.5.1.1 Man-in-the-middle (Invasor no meio da negociação SIP) 32
2.5.1.2 Quebra de senha (Ataque por dicionário) 33
2.5.1.3 Ataques de dicionário na autenticação SIP 33
2.5.1.4 Negação de Serviço (Denial of Service) 33
2.5.1.5 SIP Signalling Loop 34
2.5.1.6 Ataques Sequestro de chamadas 35
2.5.1.7 Ataques de dicionário na autenticação SIP 35
2.5.1.8 SIP Redirec 36
2.6 Segurança aos Protocolos SIP 36
2.7 Kali Linux 37
2.8 Zabbix 38

3 Trabalhos Correlatos 40

3.1 Sistema de Comunicação IP33 40

3.2 Análise de Segurança VoIP 41
3.3 Detecção de intrusão VoIP com Snort 41
3.4 Ataque de Negação de Serviço ao protocolo SIP 42
3.5 Considerações sobre os Trabalhos Correlatos35 43

4 Cenário de Testes - Iniciando os Ataques 44
4.1 Elaboração do Cenário de Testes 44
4.2 Iniciando os ataques 46

5 Experimento Dos Ataques 49
5.1 Ataque de Autenticação 49
5.2 Ataque Man-in-the-middle 52
5.2.1 Como a tabela ARP funciona? 53
5.2.2 Realizando o Ataque 53
5.3 Ataque Negação de Serviço DoS 55
5.4 Eficiência do processador e Memória nos ataques usando o Zabbix 60
5.5. Consumo de Energia nos ataques usando Zabbix 63

6 Conclusão 68

7 Referências 70

Apresentação

A preocupação com a segurança nas redes *Internet Protocol* (IP) vem crescendo exponencialmente. Medidas legais, como penas severas para criminosos virtuais, já são uma realidade. Vários estudos estão sendo realizados com intuito de explorar os problemas de segurança relacionados à VoIP.

Por outro lado, dispositivos embarcados se mostram cada vez mais eficientes com sistemas complexos e que exigem um bom desempenho. O *software* livre voz sobre IP Asterisk tem como finalidade ser uma central telefônica, uma alternativa viável para ser utilizada em dispositivos embarcados sendo possível reduzir custos e maximizar resultados.

Este livro realiza uma abordagem de segurança usando o protocolo SIP do Asterisk em plataformas embarcadas. Em paralelo, também objetiva monitorar o consumo de memória RAM, processamento e consumo de energia elétrica nos momentos de três ataques de segurança do tipo Autenticação, Man-in- the-middle e de Negação de serviço DoS.

Os resultados mostraram que o dispositivo Raspberry Pi 3 suporta de forma satisfatória os ataques de Autenticação e Man-in- the-middle , mas o sistema Asterisk, no ataque de Negação de serviço, não consegue suportar o ataque a partir de quinhentos mil pacotes enviados pelo atacante, ficando sem possibilidade de realizar chamadas tendo seu funcionamento totalmente neutralizado. Com relação ao consumo de energia notasse que o Raspberry Pi 3 em sua voltagem tende a ficar em um patamar médio de 5,19v e a Current variando entre -600,93mA a -832,41mA e o Power variando entre -3132,40mV a -4314,78mV tendo com parâmetro a quantidade de pacotes enviados pelo atacante de 0 a 25.000.000.

1 Introdução

A tecnologia *Voice Over Internet Protocol* (VoIP) consiste na integração dos serviços das áreas de telecomunicações com os serviços de redes de computadores. Assim, torna-se possível a digitalização e codificação do sinal da voz, transformando-o a voz em pacotes de dados *Internet Protocol* (IP) para a realização de comunicação em uma rede que utilize os protocolos TCP/IP.

O VoIP existe desde 1995, apresentado pelo *software Internet Phone*, que foi desenvol- vido pela empresa Vocaltech Communications. Porém, em 2003, o Skype possibilitou demonstrar ao mercado e aos consumidores a potencialidade dos aplicativos de telefonia IP (KUHN; WALSH; FRIES, 2005).

Esse novo conceito (VoIP) permite a redução dos custos de instalação, de manutenção e de gerência de redes paralelas, cada uma dedicada ao suporte de um único serviço. Ela possibilita a redução de custos, criando assim um novo conceito de telefonia, (SITOLINO, 1999) já que necessita de equipamentos, técnicas e de recursos humanos específicos (COLHER et al., 2005).

Os sistemas embarcados utilizam plataformas de *hardware*, uma vez que são dirigidos por *softwares* e diversas implementações de processadores que podem ser utilizados, o que implica uma forte redução de custos. Alguns problemas de confiabilidade são encontrados em dispositivos embarcados. Por exemplo: como não pode ser desligado com segurança para reparos, o sistema deve executar sempre, assim como modos de desempenho reduzidos não são admissíveis e o ambiente tende a apresentar perdas se for desligado (AKYILDIZ et al., 2002).

Quando se fala de VoIP, pode-se integrar vários blocos de IP diferentes a partir de fontes. Alguns IPs podem lidar com criptografia ou decodificação, enquanto outros blocos gerenciam as operações que se referem como IP de segurança *Session Initiation Protocol* (SIP). Todo IP deve atender a uma especificação de desempenho, mantendo-se dentro dos potenciais de área e tempo de colocação no mercado. O SIP

também deve ser seguro sob vários modelos de ataque, uma vez que um usuário mal-intencionado poderá tentar extrair informações do SIP de várias maneiras.

Medidas legais, como penas severas para criminosos virtuais, já são uma realidade. Os administradores de redes mais do que nunca estão implantando soluções como detecção de intrusos, *firewalls* com filtros avançados, antivírus, chaves de criptografia, proxy, entre outros. Vários estudos estão sendo realizados com intuito de explorar os problemas de segurança relacionados a VoIP. O uso de protocolos de texto, a falta de autenticação e a complexidade da implantação de segurança end-to-end sólida são apenas alguns exemplos de como as redes VoIP são suscetíveis a diversos ataques.

O atacante pode examinar fisicamente o SIP, tentar obter informações seguras durante a operação, buscar informação do ambiente de desenvolvimento ou comunicação do designer SIP ou integrador. Por isso, ameaças são considerações de segurança que devem ser levadas em consideração quando trabalhando em um projeto de configuração de utilizando-se VoIP.

De acordo com (STAPKO, 2011), segurança de computadores consiste em proteger infor- mações pessoais ou confidenciais e/ou recursos computacionais de indivíduos ou organizações que poderiam deliberadamente destruir ou se utilizar de tais informações para fins maliciosos. O chamado estado da arte em segurança na telefonia VoIP envolve a encriptação do áudio entre os dois pontos usados, interoperabilidade entre os fabricantes, servidores, criptografia indecifráveis e gerenciamento centralizado sem a necessidade de configuração (WILLIAM; STALLINGS, 2015).

Segundo (BARR; REILLY, 1999; CARRO; WAGNER, 2003), sistemas embarcados devem ser confiáveis, uma vez que falhas podem comprometer esta única função e por talvez ser difícil sua substituição remotamente.

A segurança em sistemas embarcados nem sempre foi levada em conta, uma vez que, inicialmente, a maioria deles operavam embutidos em sistemas sem conectividade com a Internet. Nesse sentido, pode-se justificar a importância da segurança da informação em novos dispositivos que estão sendo criados a partir de dispositivos embarcados, já que eles cada vez mais estão ficando presentes na vida do dia a dia. Com certeza, a comunicação entre dispositivos dará uma reviravolta na comunicação mundial, proporcionando eficiência nas comunicações VoIP.

1.1 Problemática e Hipótese

A segurança em dispositivos embarcados é uma preocupação real, tendo em vista que vários sistemas estão sendo criados a cada dia. A preocupação com a segurança é fundamental para que se possa ter a confiabilidade destes dispositivos. Segundo (JONES, 2007;MCGRAW, 2006), segurança de *software* é um tema cada vez mais relevante na medida em que muitos ataques veem explorando as vulnerabilidades deste *software*.

Para (ALHAZMI; MALAIYA; RAY, 2007), a segurança de *software* torna-se um tema central na segurança de sistemas computacionais como um todo. Já para (BARR; REILLY,1999) (CARRO; WAGNER, 2003; MARWEDEL, 2011), os sistemas embarcados são sistemas especializados, diferentemente de um elemento computacional convencional. Isso, aliado ao fato de que eles são comumente inseridos em outros sistemas, faz com que sistemas embarcados tenham suas dimensões reduzidas. Tal redimensionamento, aliado à necessidade de redução de custos, por sua vez, torna os sistemas embarcados limitados de recursos computacionais (HAMACHER et al., 2012).

Tendo em vista a implantação do Asterisk em sistemas embarcados para reduzir despesa na área de telefonia com as características de uma central telefônica, o desafio está em garantir a segurança das vulnerabilidades encontradas. Faz-se necessário, então, prover a segurança desse dispositivo contra os ataques de invasores, analisando os dados do sistema para descobrir qual foi o tipo de ataque que ocorreu. Logo em seguida, executar ações que serão planejadas e baseadas no tipo de ataque, com intuito de mitigar os possíveis danos causados ao sistema embarcado.

1.2 Objetivos

O objetivo principal deste livro é mostrar um estudo sobre segurança do sistemas Asterisk executando em plataformas embarcadas de baixo custo quando submetido a três ataques de segurança (ataques de Autenticação, Man-in-the-middle e Negação de Serviço), assim como analisar o consumo de energia, memória e uso de processamento para o sistema de comunicação de voz quando submetido a esses ataques utilizando uma placa Raspberry Pi 3.

1.3 Justificativa

O Asterisk uma solução VoIP híbrido de plataforma aberta e PABX com ótima relação custo beneficio.

Alguns dos benefícios que o Asterisk pode trazer às empresas: Integrar empresas de forma a efetuar ligações custo zero.

Nos *Call centers* o Asterisk pode ser integrado a sistemas CRM, facilitando no forneci- mento de informações a respeito de determinados tipos de clientes, fornecedores e etc...

Serviços de*voicemail,* fax e e-mail, tudo em uma única interface de gerencia web, ou seja, comunicação integrada.

Isso é só uma amostra das ferramentas que o Asterisk possui, pelo fato de ser uma plataforma livre, várias empresas estão visando desenvolver ferramentas personalizadas com o intuito de facilitar e gerenciar suas estruturas de comunicações, trazendo maior produtividade.

Ataque a servidores é um coisa rotineira, e para isto, temos sempre que monitorar e manter as políticas de segurança conforme cada serviço que roda em nossos servidores. Sempre se atualizando. Nos servidores VoIP, Asterisk, não é diferente.

A justificativa é baseada na crescente demanda em comunicação de voz e dados, bem como em tornar toda e qualquer comunicação confiável e segura, independente de ser dados ou voz, além do fato de ataques ocorrerem com frequência em redes de comunicação.

Este trabalho está pautado em realizar uma abordagem de segurança, analisar os riscos e vulnerabilidades em um dispositivo embarcado Raspberry Pi 3 com Asterisk e analisar o consumo de energia, memoria e CPU em relação aos ataques de Autenticação, Man-in-the- middle e Negação de Serviço em sistemas que usa o Asterisk.

1.4 Metodologia

A partir de trabalhos obtidos em bases reconhecidas foi realizada uma revisão bibli- ográfica visando a identificar os principais ataques em dispositivos embarcados, bem como ao protocolo SIP, no intuito de verificar o quanto se tinha de informação sobre os ataques a dispositivos embarcados (ataque,SIP).

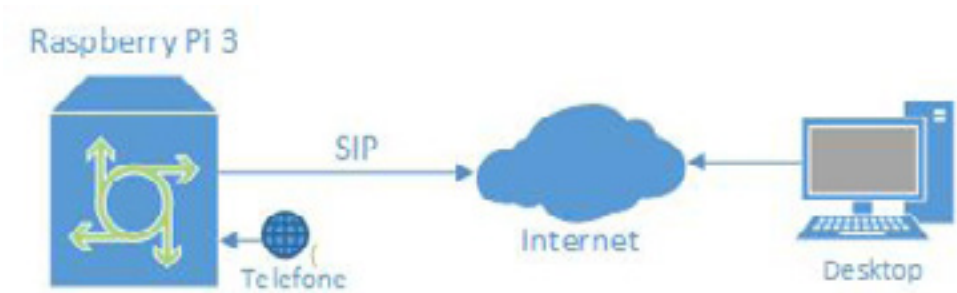
Ao aplicar esta metodologia, nota-se a importância de demonstrar como os ata-

ques a dispositivos embarcados são realizados, assim como avaliar o estado de consumo de energia no dispositivo embarcado, consumo de CPU e memória. Dessa forma, faz-se necessário seguir uma sequência para que seja possível entender os ataques de Autenticação, Man-in-middle e Ataque Negação de Serviço DOS, conforme seguinte:

- Realizar levantamento dos ataques a sistemas de comunicação;
- Realizar levantamento das ferramentas e materiais necessários para a simulação dos ataques mais significativos em dispositivos embarcados;
- Realizar revisão de literatura do protocolo SIP;
- Analisar as vulnerabilidades do protocolo SIP;
- Analisar os ataques com relação ao consumo de energia, CPU e memória
- Escrever o livro e apresentar os resultados da análise dos ataques no dispositivo embarcado Raspberry Pi 3 com Asterisks.

O estudo se inicia com a demonstração dos ataques de Autenticação, Man-in-middle e Ataque Negação de Serviço DOS, bem como com a verificação do estado de consumo de energia no dispositivo embarcado, consumo de CPU e memória, utilizando os *software* Kali Linux e Zabbix. Foi utilizado o projeto de cenário de teste conforme Figura 1.

Figura 1 – Projeto de cenário teste



Fonte: Autoria própria.

Ao término da demonstração dos ataques e coleta das informações obtidas para o estado de consumo de energia, consumo de CPU e memória, No capitulo 6 teremos as conclusõesdos resultados obtidos.

1.5 Organização do Livro

Para facilitar a navegação e melhor entendimento, este documento está estruturado em seis (6) capítulos, que são:

Na Introdução capitulo 1, apresenta o problema, justificativa e o que foi proposto neste livro. No capítulo 2 da Fundamentação Teórica, são abordados os principais temas do trabalho e tecnologias para contextualizar o leitor, com o foco em VoIP, Sistemas Embarcados, Asterisk, protocolo SIP, os principais tipos de ataques ao protocolo SIP e segurança ao protocolo SIP.

No capítulo 3 sobre os Trabalhos Correlatos, são apresentados os trabalhos relacionados ao problema descrito. No capítulo 4, são descritos o método de coleta dos dados de forma detalhada. No capítulo 5 de Experimento e Resultados, é apresentado como foram realizados os experimentos e seus resultados. Por fim, no capítulo 6, da conclusão, são abordadas as considerações dos resultados encontrados.

2
Fundamentação Teórica

2.1 VoIP

A qualidade das redes baseadas no Internet Protocol, conhecida como redes IP, tornou possível a navegação de diferentes tipos de mídia (áudio, vídeo, voz e imagens) através de uma rede que foi projetada inicialmente para o tráfego de dados.

Segundo Raake (2006), Walker e Hicks (2004), VoIP é uma tecnologia que faz a trans- missão de voz em uma rede de pacotes IP. O processo da transmissão consiste basicamente em transformar a voz analógica em digital, dividindo-a em vários pacotes e transportá-los sobre a rede IP. Após alcançar o destino, os pacotes são reorganizados e convertidos para o sistema ana- lógico novamente. O processo está cada vez mais atual com *softwares* que possuem a tecnologia, como Facebook, Messenger, Skype, Viber e WhatsApp.

O Sistema VoIP existe desde o ano de 2015, através do *software Intenet Phone* que foi desenvolvido pela (VOLCATEC, 2016). Contudo foi com o surgimento do SKYPE, no ano de 2003, que os aplicativos de telefonia IP começaram a chamar atenção das empresas e de consumidores.

Segundo a Volcatec (2016), havia a necessidade de pessoas se comunicarem, já que, naquela época, houve uma imigração de judeus da antiga URSS para Israel. Eles eram pessoas de pouco poder aquisitivo, mas que necessitavam se comunicar com suas famílias na Rússia. Acontece que a telefonia normal tinha um custo elevado, então o mercado encontrou uma forma de viabilizar um novo negócio.

Na Figura 2, podemos observar o funcionamento de uma aplicação VoIP, na qual o áudio analógico é convertido em digital e agrupado em pacotes que são transmitidos para a rede IP através do protocolo *Real Time Protocol* (RTP). Após chegar ao receptor, os pacotes são organizados e depois reproduzidos.

Figura 2 – Cenário do funcionamento ideal da aplicação VoIP.

Fonte: (RAFAEL SEIDI SHIGUEOKA, 2016).

Para podermos transmitir dados de voz são necessários componentes como codifica- dor/decodificador, protocolos TCP/IP, VoIP, *Gateways* VoIP, Roteadores, Telefones IP e *Softpho- nes*. (KELLER, 2011), aponta as principais vantagens e desvantagens do VoIP. Para um melhor entendimento, vamos comentar algumas delas.

Vantagens:

- Diminuição dos custos das ligações;
- Diminuição dos custos dos equipamentos de rede;
- Infraestrutura Única;
- Facilidade de implantação devido à larga utilização do protocolo IP;
- Integração entre voz e dados e novas aplicações;
- Melhor aproveitamento da largura de banda;
- Mobilidade;
- Mercado, lucros e empregos.

Desvantagens:

- Falta de padronização de protocolos;
- Confiabilidade e disponibilidade da rede;
- Segurança;
- Qualidade de Voz.

Segundo (GRECCO, 2004), a principal função de um sistema de comunicação é permitir que uma mensagem seja gerada por uma fonte de informação e que possa ser entregue corre- tamente ao seu destino. Para que as funções sejam executadas de forma adequada, as camadas devem obedecer às regras conhecidas e que estejam de acordo com as máquinas que participam da rede.

Essas regras, que são conhecidas como protocolos, definem o modo de operação do sistema, estabelecendo procedimentos que devem ser tomados a cada linha e que determinam o que deve ser feito a cada momento.

No sistema de telefonia, em sua inicialização, faz-se necessário estabelecer, controlar e encerrar sessões entre usuários, o que chamamos de procedimento de inicialização. Um sistema convencional possui dois tipos de sinalização: o dentro da faixa e o fora da faixa.

O sistema dentro da faixa possui esse nome por se utilizar da mesma faixa de frequência do sinal de voz que é composto de um conjunto de tons audíveis. O sistema fora da faixa, que é conhecido por sinalização em canal comum, foi criado para aumentar a eficiência do sistema de telefonia (International Telecommunications Union, 1993) e entre suas funções estão estabelecer, configurar, monitorar, rotear e encerrar as chamadas da telefonia convencional PSTN.

Os principais modelos de protocolos da rede IP são:

H.323 – Que foi desenvolvido pelo ITU-T em 1996, tendo resolvido diversos melhora- mentos e revisões até o ano de 2006, e que possui como principais protocolos o H.225, Q.931, H.245, G.7xx, RTP, RTCP, T.12x, H.450, H.26x, H.246 e H.235.

RTP – Um protocolo que possui aspectos de Qualidade de Serviço (QoS), diferenciando- se dos outros tipos de tráfego da rede e estabelecendo características que devem ser suportadas por protocolos de transporte em tempo real.

RTCP – Um protocolo que possui um protocolo próprio de controle que se chama RTCP (RTP Control Protocol), responsável por cuidar da sincronização, resposta e interface com o usuário. Esse protocolo é baseado na transmissão periódica de pacotes de controle entre seus principais participantes de sessão, através do mesmo mecanismo utilizado para distribuição de pacotes de dados.

SCTP – Protocolo que está na camada de transporte do TCP/IP e que possui

dois protocolos de transporte destinados a usos distintos. Ele permite que a flexibilidade de uma comunicação rápida e confiável recorra ao UDP. Esse é um protocolo novo que foi desenvolvido para superar as limitações impostas pelo TCP.

TCP/IP – Esse protocolo está atrelado ao desenvolvimento da Internet no ano de 1950. Seu modelo de referência surgiu como uma descrição de um conjunto de protocolos que já era encontrado em operações práticas na ARPANET.

IP – Protocolo este que mantém a inter-rede unida. Tem a função de interligar redes transportando da melhor forma possível os datagramas através da rede. Um elemento na rede IP é identificado por um endereço IP único com 32 *bits*.

TCP – É um protocolo da camada de transporte que oferece um fluxo de bytes fim-a-fim com confiança de uma inter-rede não-confiável. O TCP associa cada fluxo de dados a um par de portas que forma uma conexão ponto a ponto entre máquinas de origem e destino.

UDP – É um protocolo de transporte não-confiável e sem conexão com o TCP/IP, capaz de oferecer um meio para as aplicações enviarem datagramas IP encapsulados sem a necessidade de estabelecer uma conexão (TANENBAUM, 2003).

SIP – É um protocolo de sinalização da camada de aplicação que é utilizado para iniciar, modificar e finalizar uma sessão interativa de multimídia entre usuários. Algumas comunidades na Internet consideram esse protocolo muito melhor do que o protocolo H.323, que é muito extenso, completo e inflexível.

2.2 Sistemas Embarcados

Alguns dados pesquisados em alta tecnologia mostram que mais de 90% dos micro- computadores que são fabricados no mundo são destinados a máquinas que não são de fato computadores, como por exemplo: celulares, automóveis, aparelhos de DVD, entre outros.

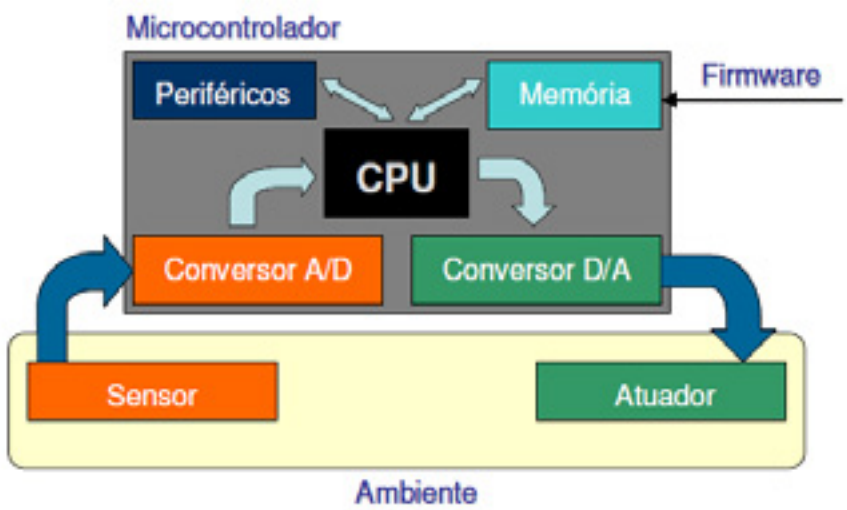
Segundo (REIS, 2004), o que vem a diferenciar o conjunto de dispositivos de um compu- tador é o projeto baseado em um conjunto dedicado e especialista, constituído por *Hardware*, *Software* e Periféricos, ou seja, Sistemas embarcados.

Segundo (CUNHA, 2007), O termo embarcado significa que uma unidade de micro- processamento está encapsulada e a serviço de uma tarefa específica. “Colocar capacidade computacional dentro de um circuito integrado, equipamento ou sistema”.

Em 1970, o mundo ganhava mais um marco simbólico, o Air Data Central Computer (CADC), que foi o primeiro sistema baseado em microprocessadores e que tinha como função o controle de uma central de voo. Já nos anos 80, o mercado estava com circuitos que combinavam microprocessador, RAM e dispositivos de Entrada/Saída. Eles eram mais acessíveis, porém não muito flexíveis como os computadores convencionais.

Para (BALL, 2005), o sistema é classificado como embarcado quando ele é dedicado a uma única tarefa e interage continuamente com o ambiente à sua volta, por meio de atuadores e sensores. Na Figura 3, demonstramos um diagrama básico de um sistema embarcado dotado de um micro controlador e uma variável “ambiente” como temperatura e umidade de uma sala.

Figura 3 – Diagrama básico de um sistema embarcado dotado de um micro controlador monito- rando o ambiente.



Fonte: (CHASE, 2007)

No artigo (SIQUEIRA et al., 2006), o autor comenta sobre o uso de sistemas embarcados em aplicações críticas. Aplicações críticas são aquela em que os riscos associados aos perigos envolvidos são considerados inaceitáveis e precisam ser tratados.

O sistema embarcado comumente é uma solução formada de microcontrolador e *software (firmware)* dedicados e específicos para desempenhar as funções operacionais de um equipamento para o qual foi projetado.

2.3 Raspberry Pi 3

Em 2006, Eben Upton, Rob Mullins, Jack Lang e Alan Mycroft resolveram criar um computador pequeno e acessível para crianças no laboratório da University of Cambridge, na Inglaterra. Eben Upton, diretor de Estudos em Ciência da Computação na universidade, havia observado que os alunos que se candidatavam a participar do laboratório de Ciências da Computação da Universidade não apresentavam as mesmas habilidades e domínio das máquinas que tinham os alunos da década de 1990.

Naquela época, jovens de 17 anos que desejavam cursar essas disciplinas já chegavam à faculdade com conhecimento de linguagens de programação e do funcionamento do *hardware;* alguns até trabalhavam com a linguagem Assembly1.

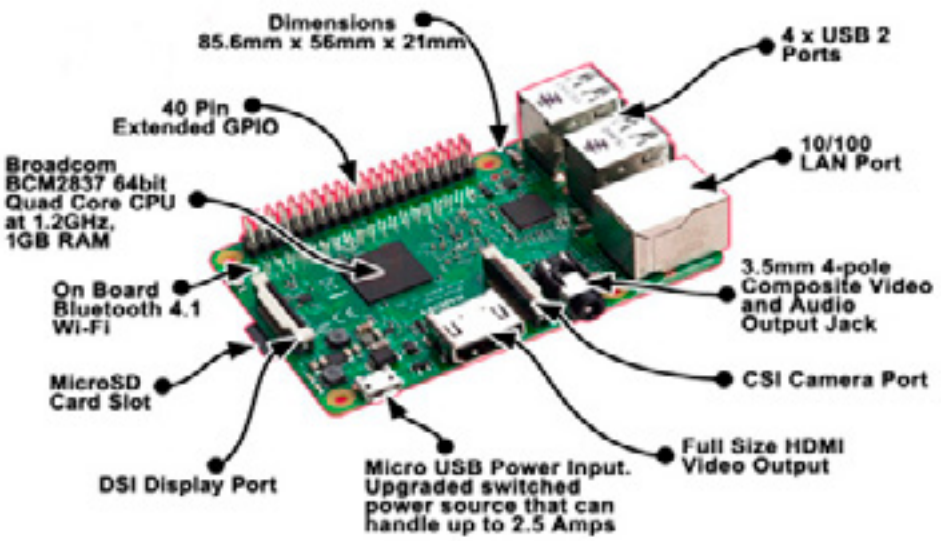
O primeiro protótipo do pequeno computador surgiu na mesa da cozinha da casa de Eben. Ele e seus amigos começaram a soldar, em uma protoboard2 com um chip Atmel3 e alguns outros chips baratos de microcontroladores4 para monitorar um aparelho de TV. O projeto contava com apenas 512 K de memória RAM, atingindo poucos MIPS5 de processamento.

O Raspberry Pi 3 se trata de um dispositivo embarcado que possui processamento considerável, devido ao processador Broadcom BCM2837 de 64 *bits* e *clock* de 1.2GHz. Com *Wifi* e *Bluetooth* 4.1 integrados, ele evita que o usuário compre adaptadores adicionais, o que deixa as portas USB livres para serem utilizadas por outras aplicações.

A placa possui 1G de memória RAM, adaptador para cartão microSD e GPU Videocore IV 3D. É uma placa que possui compatibilidade com o modelo anterior, Raspberry Pi 2, não só em termos de aplicações como também em seu *layout*, já que os seus conectores foram mantidos na mesma posição, assim como o tamanho e a perfuração

da placa. Com a Raspberry Pi 3, é possível executar diversas distribuições Linux como o Raspbian e Ubuntu, além do Windows 10 IoT. A Figura 4 ilustra a placa Raspberry Pi 3.

Figura 4 – Raspberry Pi 3.



Fonte: Adaptado de Zapals (2018).

2.4 Asterisk

O Asterisk, segundo (DASTERISK, 2016), é um *software* que emula funcionalidades de sistema de comunicação de voz. Ele foi criado e vem se aprimorando na mesma metodologia do Linux, por base de usuários em constante crescimento. O *software* foi desenvolvido inicialmente por Mark Spencer com o objetivo de criar uma PABX sobre IP que satisfaz as necessidades das empresas.O código do Asterisk é aberto, podendo ser manipulado por qualquer usuário, o que possibilita uma infinidade de configurações e a realização de mudanças de forma rápida. O grande conjunto de opções de configurações e o código aberto permite um alto grau de adaptação às necessidades das empresas e usuários.

O Asterisk é utilizado em conjunto com o VoIP e, aliado a uma Internet rápida, permite uma conexão praticamente sem limites, possibilitando que empresas se comuniquem com seus escritórios ou funcionários em diversas partes do mundo com um custo baixo e com qualidade de serviço. Entre algumas funcionalidades que estão presentes em um sistema de comunicação, o Asterisk também suporta chamadas em espera, identificação do usuário e redirecionamento de chamadas. Podemos destacar outros recursos que não são oferecidos pelas operadoras, mas que o Asterisk oferece:

- Tronqueamento – Uma funcionalidade que permite acesso de vários usuários a um número irrestrito de linhas de comunicação. O tronqueamento permite ainda um compartilhamento tanto de acesso à rede telefônica pública quanto para o acesso a canais de comunicação privados;
- Distribuição de chamadas – para receber uma chamada, o Asterisk pode se utilizar de alguns atributos predefinidos e encaminhar as chamadas com mais rapidez ao seu destino, podendo ainda encaminhar uma chamada para um único usuário ou para um grupo de extensões que tocarão em uma ordem predefinida até que ela seja atendida.
- Gravação do histórico – Possibilita o armazenamento detalhado de cada chamada realizada com o mês, dia e horário da ligação, assim como o tempo da ligação, origem da ligação etc;
- Gravação de chamadas – É possível através do Asterisk a gravação de toda conversa tanto recebida como discada, possibilitando que uma empresa possa verificar o tipo de atendimento que seu funcionário está prestando aos seus usuários;
- *Interactive Voice Response* – Um recurso amplamente utilizado em call centers, o que possibilita robotizar o atendimento com voz, levando o usuário às informações ou ramais desejados;
- Correio de Voz – Podem ser realizadas configurações individualizadas. É possível ainda a notificação de novas mensagens no correio de voz via e-mail, podendo anexar sua própria mensagem de voz.

(GROSS, 2011), em seu livro "VoIP com Asterisk", coloca que o Asterisk, em sua arquitetura, foi desenvolvido para máxima flexibilidade. Suas APIs específicas são determinadas em volta de um avançado núcleo, que é um sistema de comunicação. Sendo assim, o núcleo faz a interação entres as APIs do sistema para que seja possível executar de forma simultânea e conectada às funções que se espera do *software.*

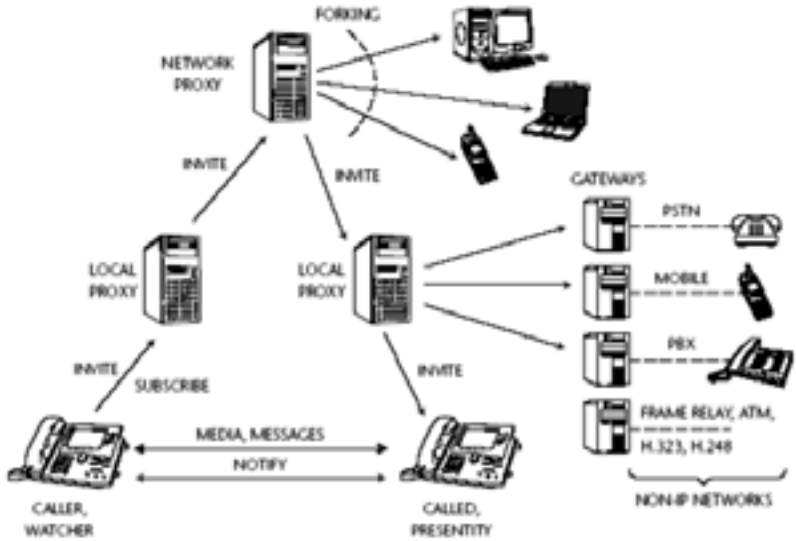
2.5 Protocolo *Session Initiation Protocol* (SIP)

O SIP foi desenvolvido a fim de facilitar a implementação dos aspectos básicos de uma sessão, que é um processo nada trivial. Hoje é utilizado em escala mundial e é também um forte "concorrente" do H.323. (BARBOSA, 2006) define SIP como um protocolo que sinaliza sessões cliente-servidor destacando presença e mobilidade, tendo como primitivas inicialização, modificação e finalização de sessões.

Segundo (DEFSIP, 2006), Juntamente com RTP (*Real-time Transport Protocol*), RTSP (*Real Time Streaming Protocol*) e o SDP (*Session Description Protocol*), o SIP estabelece uma arquitetura multimídia completa, provendo serviços completos ao usuário. Por (GROSS, 2011), o protocolo SIP se parece com o protocolo HTTP, sendo também um protocolo que se baseia em texto e que funciona como cliente/servidor, implementando métodos de requisição e resposta na comunicação. Segundo (KELLER, 2011), o SIP é um protocolo de sinalização simples, modular e escalável de realizar chamadas de voz. Vale ressaltar ainda que esse protocolo é o único módulo projetado para interoperar bem com as aplicações da Internet.

O SIP deve proporcionar serviços de gerenciamento de participantes de uma seção. Segundo (CUERVO et al., 2000), por ter essa capacidade de trabalhar em conjunto com outros protocolos, ele permite que haja a integração com a telefonia pública, permitindo não só a ligação entre ramais IP, como também para telefones de rede pública. Os aspectos de segurança do SIP fornecem particularidades que incluem prevenção de negação do serviço, autenticação, integridade e serviços privados e encriptação. Na Figura 5, temos uma visão geral do protocolo SIP com o estabelecimento das sessões e uma arquitetura formada por agentes de usuários e servidores SIP.

Figura 5 – Visão geral SIP



Fonte: (SINNREICH, 2006)

Para (MINOLI, 2002), o SIP promete ser um protocolo das redes de comunicação con- vergentes. O seu desenvolvimento teve como foco os aspectos de intratabilidade com protocolos existentes da IETF (Internet Engineering Task Force), escalabilidade, simplicidade, rapidez, mobilidade e facilidade na implementação das características e serviços.

2.5.1 Tipos de ataques aos Protocolos SIP

2.5.1.1 Man-in-the-middle (Invasor no meio da negociação SIP)

Para esse ataque, o invasor pode utilizar duas técnicas: envenenamento da tabela ARP ou clonagem do DNS. Com qualquer uma delas, se consegue a permissão para estar entre o servidor SIP e o Agente Usuário. Com esse tipo de ataque, o intruso não precisa necessariamente conhecer usernames e passwords válidos; basta rotear o tráfego entre servidor e cliente e depois agir interceptando os pacotes, impedindo-os de chegar ao seu destino real, que é o servidor SIP. (NAKAMURA; GEUS, 2007)

2.5.1.2 Quebra de senha (Ataque por dicionário)

O protocolo SIP envia a sua senha de autenticação utilizando o algoritmo de desafio MD5. O invasor, por sua vez, pode capturar os pacotes na rede utilizando um programa de mercado comum, como por exemplo o Wireshark, para capturar dados como o usuário. Quando o ataque for feito, ele já terá os dados necessários para efetuar a investida com sucesso já na primeira vez, eliminando as chances de medidas corretivas por parte do administrador da telefonia IP.

2.5.1.3 Ataques de dicionário na autenticação SIP

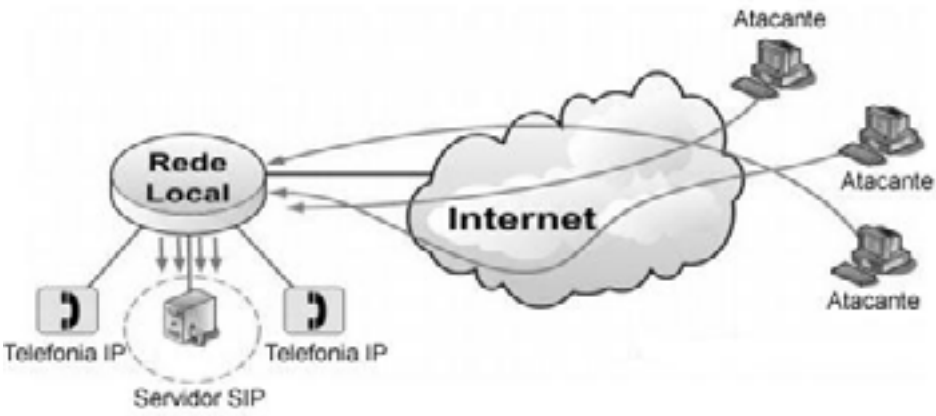
Segundo (THERMOS, 2007), esse ataque tem como objetivo obter credenciais de usuá- rios válidos em um sistema de comunicação de telefonia SIP, utilizando-se de um ataque de força bruta, ou seja, enviando várias requisições de registro com identificação (IDs) e senhas a partir de um dicionário.

2.5.1.4 Negação de Serviço (Denial of Service)

Nos ataques conhecidos como negação de serviços, ou pelo acrônimo DoS (Deniel of Service), pode-se direcionar para camadas de infraestrutura em ambiente VoIP. Segundo (THERMOS, 2007)), os ataques DoS têm como principal objetivo provocar a interrupção do serviço alvo. Nesse caso, o ataque é direcionado tanto para o sistema operacional quanto para os serviços de rede. Essa é uma ameaça que gera muita preocupação para as empresas (THERMOS; ARI, 2008).

Os tipos de ataque de negação de serviço comum, conforme Figura 6, são os de inundação que consistem em enviar uma sobrecarga de mensagens para um único destino, provocando o mau funcionamento e o pacote deformado, conhecido como processo Fuzzing. Ele gera pacote deformado aleatoriamente, provocando um comprometimento do dispositivo alvo.

Figura 6 – Ataque de negação de serviço em servidor SIP Fonte: (Brito S. H. B, 2011)



Fonte: (Brito S. H. B, 2011)

O ataque de negação de serviço a um sistema VoIP é fácil de ser realizado em redes que não são bem preparadas, pois, por ser um tipo de aplicação em tempo real, o VoIP é particularmente sensível ao excesso de tráfego que pode ser gerado intencionalmente por um vírus, por exemplo (THERMOS; ARI, 2008).

O alvo de ataques de negação de serviço pode ser qualquer coisa no caminho da men- sagem, incluindo as defesas de perímetro, o proxy SIP, ou o agente usuário (UA). O ataque também pode ser lançado a partir da rede PSTN *(Public Switched Telephone Network)* ou pode ser orientado para uma rede PSTN por trás de um proxy VoIP (THERMOS; ARI, 2008).

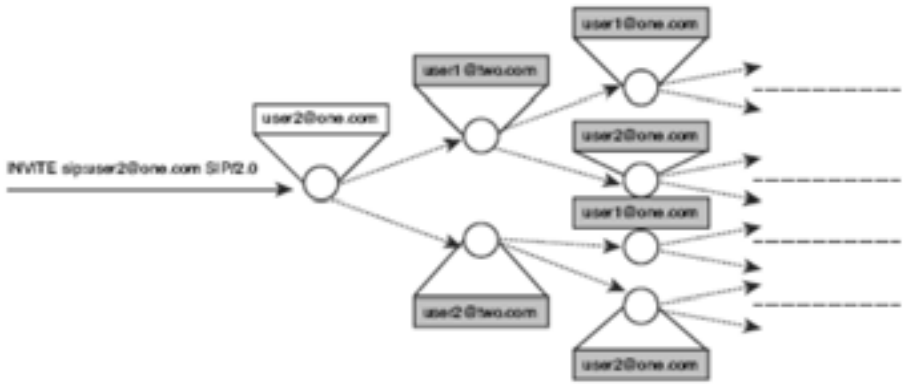
Qualquer interface de comunicação aberta pode ser inundada. Os melhores alvos para a inundação são as portas estáticas, como 5060 (TCP e UDP) de SIP e porta 1720 (TCP) para H.323/H.225 inicial de sinalização (THERMOS; ARI, 2008)

2.5.1.5 SIP Signalling Loop

Esse tipo de ataque, conforme Figura 7, segundo (THERMOS, 2007), afeta o sistema que não implementa mecanismo de detecção de looping. O ataque consiste em registrar dois usuários em um domínio SIP distinto, colocando dois valores no cabeçalho de contato, cada um apontando para um desses usuários em domínio contrário. Quando o SIP Proxy em um domínio recebe o INVITE para um desses usuários

ele gera duas mensagens de INVITE sendo uma para cada usuário de outro domínio. No SIP Proxy do outro domínio por sua vez, ao receber esses dois INVITE's irá gerar quatro novas mensagens de INVITE para outro domínio. Sendo assim, o número de mensagens irá crescer em ordem de uma potência de base dois e rapidamente poderá comprometer o sistema SIP (THERMOS, 2007).

Figura 7 – SIP Signalling Loop



Fonte: (THERMOS, 2007)

2.5.1.6 Ataques Sequestro de chamadas

Para esse ataque, em (THERMOS, 2007), no cabeçalho de requisição chamado de Register, no sistema SIP, existe um registro com informações de contato que é usado pelo Prox do SIP para rotear ligações ao dispositivo do usuário, podendo ser realizado o ataque através da alteração das informações do endereço IP contidas no registro.

2.5.1.7 Ataques de dicionário na autenticação SIP

Segundo (THERMOS, 2007), esse ataque tem como objetivo obter credenciais de usuá- rios válidos em um sistema de comunicação de telefonia SIP, utilizando-se de um ataque de força bruta, ou seja, enviando várias requisições de registro com identificação (Ids) e senhas a partir de um dicionário.

2.5.1.8 SIP Redirec

Para (BUTCHER; LI; GUO, 2007), o ataque emprega um servidor que recebe solicitações de um telefone ou Prox e retorna uma resposta de redirecionamento indicando onde o pedido deve ser repetido. Isso permite que o usuário tenha uma chamada onde o telefone toca diferente de onde está localizado, sendo que o chamador só marca um único número para chegar ao usuário. O atacante redireciona as chamadas da vítima para um número específico de sua escolha, sendo assim, ele pode receber chamadas que foram encaminhadas para o usuário atacado.

2.6 Segurança aos Protocolos SIP

Um sistema de comunicação configurado de maneira errada pode deixar brechas de segurança, proporcionando falhas nas configurações do plano de discagem, e, assim, liberando aplicativos para usuários internos e externos que não possuem autorização de acesso. Quando se desabilitam rotas que não são essenciais para o funcionamento de um sistema de comunicação, evitam-se esses e outros tipos de problemas cuidando da segurança, bem como tomando cuidados em configurações para não proporcionar esses tipos de invasões e emprego não autorizado dos sistemas de comunicação.

Segundo (GROSS, 2011), alguns cuidados devem ser tomados para evitar acessos inde- sejados, assim como ter um maior controle de quais rotas ou ramais podem ou não ser acessados, além do segmento de classes das extensões em diferentes contextos e trabalhar com as inclusões entre eles. Quando for utilizar URAs, tem que ter a certeza de que as ligações que entram por ela tenham seu acesso controlado e não se utilizem do sistema de comunicação. Devemos ter cuidado com o default do Asterisk, pois sempre que uma extensão não for encontrada, a mesma será direcionada para o contexto padrão.

Para (Brito S. H. B, 2011), o protocolo SIP deve oferecer confiabilidade de maneira que somente usuários autorizados possam ter acesso às informações que estão sendo transmitidas, pois o sigilo das ligações deve ser mantido. Outra característica é a integridade das seções do SIP, que deve garantir que as seções sejam mantidas até que uma das partes solicite formalmente a desconexão.

Segundo (YOSHIOKA, 2003), para que se possa prover segurança para a rede

SIP, podemos utilizar o IPSec, S/MIME e TLS, pois o IPSec proporciona a capacidade de comunica- ção segura entre os pontos através do estabelecimento de uma rede virtual (VPN). O S/MIME concede a segurança de conteúdo, utilizando-se da criptografia do conteúdo das mensagens SIP, que, por sua vez, se utiliza da tecnologia RSA (Rivest-Shamir-Adleman), a qual é uma metodologia segura para emitir um e-mail, mas também para promover segurança ao SIP. O TLS (Trasnport Layer Securit) propõe uma camada segura de transporte que envolve o TCP.

2.7 Kali Linux

Segundo (HERTZOG;; O'GORMAN;; AHARONI, 2012), o projeto KaliLinux começou em julho de 2012, quando a Offensive Security decidiu substituir o projeto venerable black track linux, que foi mantido manualmente e poderia ser usado como Debian derivative3, com o intuito de concluir o trabalho de infra-estrutura e melhorar as técnicas de pacotes.

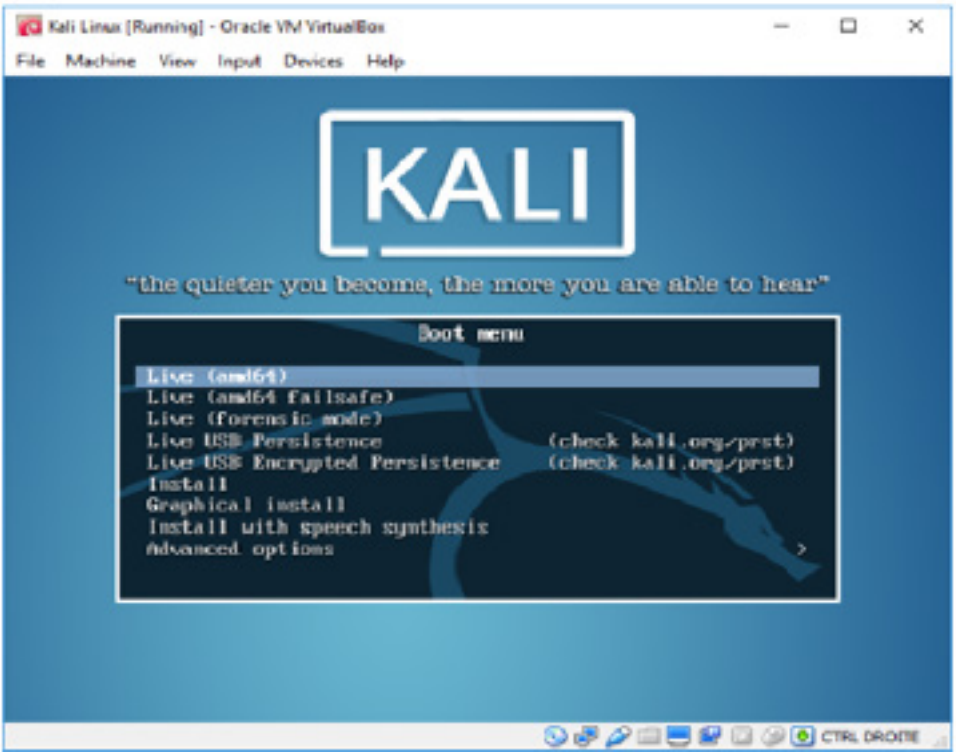
A decisão foi a de criar o Kali on top da distribuição Debia, porque ela é conhecida por sua qualidade, estabilidade e ampla seleção de *software* compatível. O primeiro lançamento (versão 1.0) aconteceu um ano depois, em março de 2013, e foi baseado no Debian 7 "Wheezy", a distribuição estável do Debian na época.

Nesse primeiro ano de desenvolvimento, foram empacotados centenas de aplicativos relacionados, assim como construída a infraestrutura. Nesta versão, o número de aplicativos foi significativo e uma lista de aplicativos foi cuidadosamente selecionada. Durante os dois anos após a versão 1.0, Kali lançou muitas atualizações incrementais, expandindo assim a gama de aplicações disponíveis e melhorando o suporte de *hardware,* graças às novas versões do kernel.

A distribuição do Kali Linux é baseada no teste do Debian 9. Portanto, a maioria dos pacotes disponíveis no Kali Linux tem a visão deste repositório do debian. Embora o kali Linux seja totalmente independente da infraestrutura e mantém a liberdade de mudanças.

A Figura 8 mostra a tela de inicialização do Kali Linux no Virtual Box.

Figura 8 – Assistente de Máquina Virtual



Fonte: (HERTZOG;; O'GORMAN;; AHARONI, 2012)

2.8 Zabbix

O Zabbix foi elaborador por Alexei Vladishev, e atualmente ele é mantido e pela Zabbix SIA. O Zabbix é uma solução de nível enterprise, com código aberto e com suporte a monitoração da distribuída. Segundo (Dalle Vacche; Kewan Lee, 2015), o Zabbix surgiu em 2001 e desde o seu lançamento se distinguiu como uma solução de monitoramento poderosa.

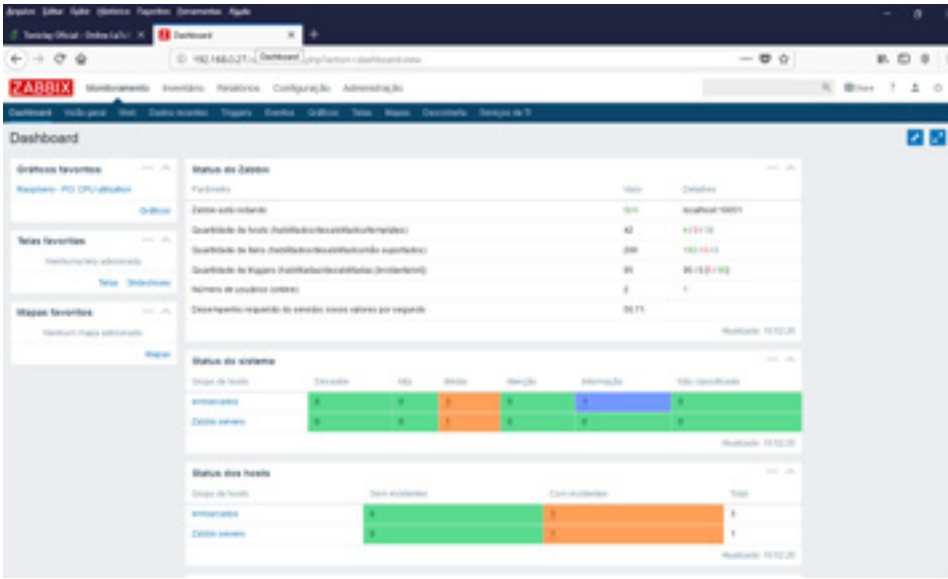
O Zabbix é um *software* que monitora vários procedimentos da rede, dos servidores e de seus serviços. Utiliza-se de um mecanismo flexível de notificação que permite configurar alertas através de e-mail em seus eventos, alertando assim seu administrador. As notificações permitem que rapidamente os problemas no ambiente sejam resolvidos. O Zabbix também oferece recursos de relatórios e visualização

de dados armazenados. Isso faz com que o Zabbix seja uma ferramenta de planejamento de capacidade.

Os relatórios e estatísticas do Zabbix, e seus parâmetros de configuração, estão sempre disponíveis em interface web. O uso desta interface web garante que se possa avaliar o estado de sua rede e de seus servidores a partir de qualquer local. Quando corretamente configurado o Zabbix desempenhar um papel importante na infraestrutura de monitoramento de TI. Estas características se aplicam as empresas de pequeno e grande porte.

Zabbix é um *software* consolidado como ferramenta de monitoramento em redes de computadores, servidores e serviços. O mesmo possui o intuito de monitorar a integridade, disponibilidade, experiência de usuário e qualidade de serviços. A figura 9 demonstra a interface do *software* Zabbix.

Figura 9 – *Software* Zabbix.



Fonte: Autoria própria.

3
Trabalhos Correlatos

Os trabalhos abordados nesta pesquisa contêm um grande número de referências. Dessa forma, utilizou-se a Base do IEEE com estudos realizados entre 2012 e 2016, com foco nas palavras-chaves (VoIP, Asterik, SIP, Segurança).

3.1 Sistema de Comunicação IP

O artigo (LOMOTEY; DETERS, 2014) mostra que os sistemas de comunicação IP têm sido alvo de ataques como roubo de chamada e ataques a servidores, o que possibilita acesso aos dados dos usuários. Sendo assim, o autor propôs uma solução para prevenir o acesso de atacantes ao sistema de telefonia construído em Asterisk. Em seu experimento, não se utilizou uma plataforma completa para o Asterisk, pois ele propôs um middleware baseado em nuvem, camada esta que mantém a parte mais sensível da chamada de informações.

O Asterisk foi utilizado para as discagens, chamadas, roteamento e recebimento das chamadas. O middleware utilizou-se do padrão REST para interação com o Asterisk. O sistema comunicação IP é uma tecnologia adotada na maioria das empresas para gerir a telefonia, permitindo uma comunicação intraoffice, que é a comunicação com entidades empresariais externas. Neste trabalho, os autores propuseram um sistema comunicação IP distribuído e baseado na tecnologia Asterisk para auxiliar na marcação de clientes com monitoramento mínimo dos empregados no call center. Foram utilizadas as ferramentas Fail2Ban e Snort como medidas para verificar as limitações de ataque, pois a escalabilidade do sistema Asterisk vem sendo posta em questão quando está sob ataque.

O ataque DoS na primeira experiência foi avaliado por três meses em cenário real, onde foram identificados cerca de 25.241 ataques com o intuito de inundar os servidores Asterisk, tornado-os inacessíveis. Foram detectados 39.689 ataques de identidade falsa os quais envolveram a emissão de credenciais falsas na tentativa de

entrar no sistema e realizar milhares de chamadas quando esse tipo de ataque era realizado em empresas. Tendo em vista os ataques mencionados, os autores propuseram a camada de middleware para coordenar todas as atividades do sistema, armazenamento dos dados em SQL e empacotamento de marshaling no middleware para prevenir o roubo de informações.Os autores concluíram que o experimento teve sucesso nos ataques Denial of Service (DoS), que são ataques de identidades falsas e ataques de sondagem. Foi avaliado ainda o desempenho do sistema contra inundações, que mostrou um aumento de alto desempenho. Este trabalho ainda sugere como estudo futuro a exploração da expansão no discador preditivo onde se misturam a discagem preditiva e a discagem automática.

3.2 Análise de Segurança VoIP

Em (REHMAN; ABBASI, 2014)), o termo VoIP é utilizado para a comunicação que fornece dados de voz e multimídia utilizando-se da Internet que, devido à sua popularidade, tornou-se alvo de diversos ataques.

No artigo em questão, o autor analisou a segurança na arquitetura VoIP no sistema de comunicação de voz sobre IP Asterisk. Percebendo que a maioria dos ataques estavam relacio- nados à fragilidade do protocolo SIP, foram detectados ataques de espionagem, modificação e interrupção involuntária.

No estudo, foi proposta, para resolução do problema apresentado, a necessidade de o protocolo SIP de fornecer um mecanismo de autenticação eficiente e seguro, garantindo assim uma maior proteção aos ataques.

Foi sugerido ainda atribuir um token criptográfico que autenticaria os usuários, possibili- tando a identificação do utilizador e proporcionando uma maior segurança. Assim não existiria a necessidade do usuário de colocar a senha para utilizar outros serviços disponíveis.

3.3 Detecção de intrusão VoIP com Snort

No artigo de (ČÍŽ et al., 2012), os autores descrevem alguns tipos de ataque em tráfego de VoIP e apresentam formas de proteção contra eles. Em seu experimento, foi proposto um modelo focado em ataque DoS com o objetivo de causar um mau funcionamento no Asterisk. Foi utilizado o SIPp, ferramenta usada para verificar

a funcionalidade do sistema de detecção e causar anomalias em ataques de negação de serviço, bem como a ferramenta de *software* Snort, usada para a detecção de ataque em rede livre, e de sistemas de prevenção capazes de realizar análise do tráfego e log de pacotes em redes IP utilizadas.

O artigo foi organizado pelas descrições dos tipos de ameaças em VoIP, uma proposta de modelo de proteção IDS com experiência, finalizando com explicação dos resultados encontrados. O tráfego foi controlado através do intercâmbio do Asterisk, criando regras definidas focadas em negação de serviços. O objetivo do trabalho futuro é encontrar outras variantes de regras de negação de serviço e avaliar a sua eficácia, eventualmente, para se concentrar em outro tipo de ataque.

3.4 Ataque de Negação de Serviço ao protocolo SIP

O artigo de (BANSAL; PAIS, 2015), apresenta-se o protocolo SIP como sendo o mais popular usado em protocolo VoIP e propõe um esquema de mitigação para SIP em sistemas VoIP para protegê-lo de inundações de ataques DoS.

Os autores criaram um protótipo para criar inundação de ataques DoS baseado em um servidor SIP para avaliar o desempenho do sistema proposto, no qual realizaram um total de 167 chamadas, significando que 167 canais ficaram disponíveis no servidor SIP no esquema de mitigação. A ferramenta SIPp foi executada em 10 terminais, onde cada um emitiu 1000 mensagens CONVIDADOS e o número de terminais foi aumentando um por um, ao tempo em que foram enviadas 1000 * 10 mensagens INVITE, tendo como resultado canais ocupados no servidor Asterisk .

Sendo assim, antes de implementar o esquema de mitigação, apenas uma atacante poderia envolver todos os canais SIP enviando apenas 200 INVITE mensagens no servidor SIP. Após a implantação do esquema proposto, foi identificado um usuário atacante que começou a descartar todas as mensagens INVITE recebidas, bem como parou de enviar mensagens BYE para o atacante desprender todos os canais que foram ocupados por ele inicialmente.

Os autores concluíram que o plano de mitigação proposto atingiu o seu objetivo de proteger o servidor SIP de ficar caindo e fornecendo o serviço a todos os novos usuários legítimos durante um ataque de negação de serviço (DoS).

3.5 Considerações sobre os Trabalhos Correlatos

A tabela 1 ilustra a comparação entre os trabalhos correlatos, demostrando a utilização de *hardware, software,* protocolo, desempenho e se é um experimento. Podemos verificar na tabela 1 (BANSAL; PAIS, 2015), que é realizada uma avaliação de um ataque de negação de serviço em um computador com protocolo SIP. Trata-se de caso semelhante ao nosso, com a diferença de que utilizamos um Raspberry Pi 3 em um ataque de negação de serviço e testamos o Raspberry Pi 3 em mais dois ataques, além de coletar os resultados de consumo de energia bem como o comportamento da memória e CPU.

Podemos observar que dois estudos se utilizam do protocolo IP e dois do protocolo SIP, sendo os dois trabalhos IP: (LOMOTEY; DETERS, 2014) e (ČÍŽ et al., 2012) verificam o desempenho contra inundações de DoS e a análise do tráfego com os logs de pacotes; (REHMAN; ABBASI, 2014) e (BANSAL; PAIS, 2015) analisam a eficiência da segurança e avaliam um esquema de mitigação para SIP em sistemas VoIP com o intuito de protegê-los de inundações dos ataques DoS.

Tabela 1 – Comparação entre os trabalhos correlatos.

Autores	Tema	Hard	Soft	Prot	Desemp	Exper
(LOMOTEY; DETERS, 2014)	Sistema de comunicação IP	X	Asterisk Fail2 Ban2 Snort	IP	Contra inundações DoS	X
(REHMAN; ABBASI, 2014)	Análise de Segurança VoIP	X	Asterisk	SiP	Eficiência de Segurança	X
(ČÍŽ et al. 2012)	Detecção de intrusão VoIP com Snort	X	Asterisk, Snort	IP	Análise de tráfego e log de pacotes	X
(BANSAL; PAIS, 2015)	Ataque de negação de serviço ao protocolo SiP	X	Asterisk	SiP	Avaliar	X
Esta Dissertaçao	Uma Abordagem de Segurança do Sistema Asterisk em Plataformas Embarcadas usando o Protocolo SiP	X	Asterisk Zabbix Wireshark x-lite VM Virtual Box	SiP	Análise de ataque	X

Fonte: Autoria própria.

4
Cenário de Testes - Iniciando os Ataques

Este capítulo apresenta a implementação do experimento, que consiste em: realizar a montagem do cenário de teste com o dispositivo embarcado Raspberry Pi 3; efetuar a abordagem dos *softwares* necessários no dispositivo para a elaboração do experimento de invasão, seguindo a logica de primeiramente levantar a topologia da rede do servidor a ser at acado; e montar os três tipos de ataque na seguinte ordem :

- Ataque de Autenticação;
- Ataque Man-in-middle;
- Ataque Negação de Serviço DOS.

Nos ataques são realizados os monitoramentos do consumo do processamento, memória e energia, tendo como objetivo avaliar o dispositivo embarcado Raspberry Pi 3 e o *software* Asterisks.

4.1 Elaboração do Cenário de Testes

Ao realizar o cenário de teste foi necessário instalar um sistema operacional no dispositivo embarcado, utilizando Raspbian no Raspberry Pi 3, sistema operacional este baseado no GNU Linux Debian 8.

Em sequência, ocorreu a instalação do *software* de comunicação por voz sobre IP Asterisk. Por último foi instalado um dissipador de calor, assim como um *cooler*, a fim de refrigerar os dispositivos. Isso porque houve um elevado número de ocorrências das mensagens de alarme referindo-se à alta temperatura no dispositivo.

Foi necessária a instalação de duas máquina virtuais utilizando o Oracle VM VirtualBox: uma com o Kali Linux, para realizar o ataque, e outra com *software* de monitoramento Zabbix, para capturar o processamento e memória do Raspberry Pi 3 na hora de realização dos ataques. A Tabela 2 ilustra os *softwares* utilizados no experimento

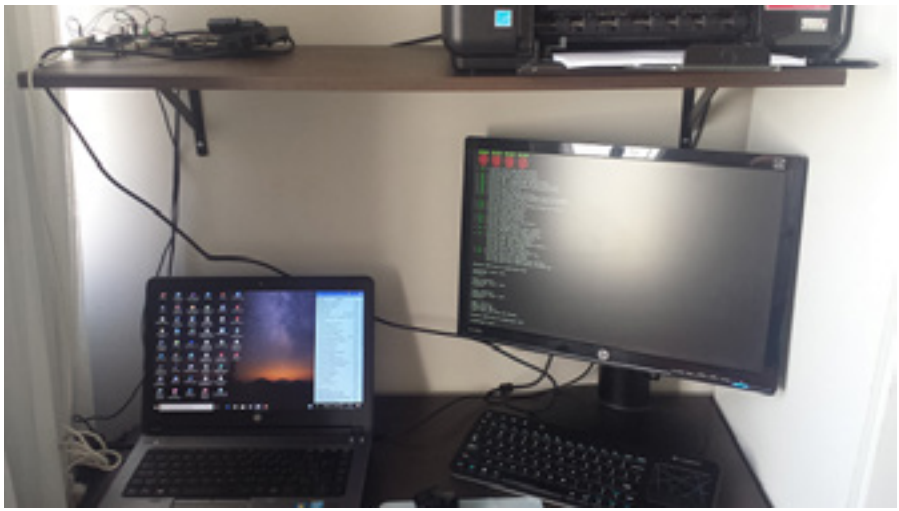
Tabela 2 – Software utilizados no experimento.

Dispositivos	*Notebook*	VM VirtualBox
Raspberry Pi3 Asterisk 13	Sistema de comunicação IP	Asterisk 13 Zabbix Kali Linux

Fonte: Autoria própria.

A intenção é verificar o comportamento do Raspberry Pi 3, juntamente ao *software* de comunicação voz sobre IP Asterisk, bem como verificar o status do processamento, memoria e consumo de energia durante os ataques propostos, utilizando o *software* Zabbix; acompanha- mento do consumo de energia com o circuito INA219. A Figura 10 ilustra o cenário real em que os testes foram realizados.

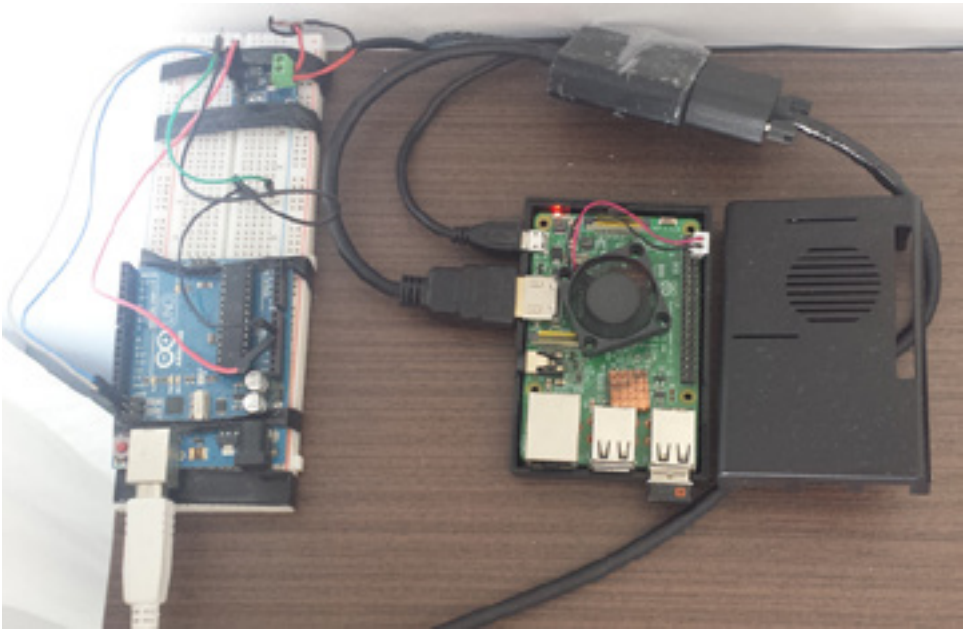
Figura 10 – Cenário real de testes.



Fonte: Autoria própria.

A Figura 11 mostra o Raspberry Pi 3 e o circuito INA219 medidor de energia.

Figura 11 – Raspberry Pi 3 e o circuito INA219 medidor de energia.



Fonte: Autoria própria

4.2 Iniciando os ataques

Para inciar os ataques com o Kaki LInux no Raspberry Pi 3, juntamente ao Astrerisk, foi necessário verificar inicialmente a topologia da rede na qual realizamos o ataque. Para isso, foi preciso:

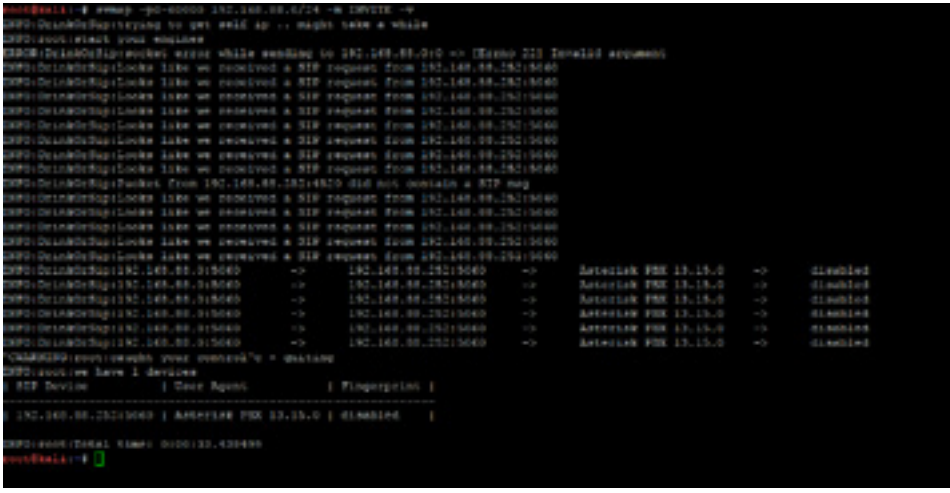
- Verificar a faixa de Ip;
- Versão da aplicação;
- Extensões.

Sendo assim, o atacante faz uma varredura dos ip's e portas em uma rede com o comando no kalli Linux, para fazer a varredura conforme Figura 12:

Para realizarmos a varredura da rede a ser atacada, usamos o comando no Kali Linux abaixo.

```
# svmap -p0-60000 192.168.0.0/24 -m INVITE –v
```

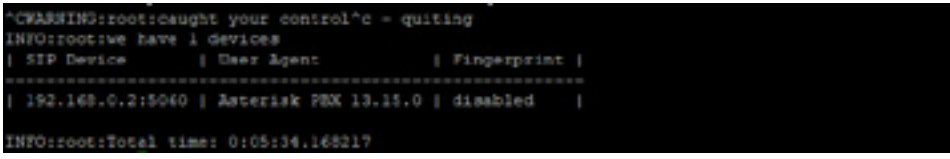
Figura 12 – Varredura de rede através do comando smvmap



Fonte: Autoria própria.

Tendo como resultado o IP e a versão da aplicação conforme Figura 13.

Figura 13 – Resultado da Varredura de rede através do comando smvmap



Fonte: Autoria própria.

Para que pudéssemos identificar uma extensão no Kali Linux, usamos o comando abaixo:

```
# svwar 192.168.0.2 –force
```

Na Figura 14 mostra a existência de um ramal com a extensão 100.

Figura 14 – O atacante identifica uma extensão, a extensão 100.

Fonte: Autoria própria.

Concluindo esta primeira etapa, podemos agora realizar os ataques.

5
Experimento Dos Ataques

5.1 Ataque de Autenticação

O protocolo de iniciação de sessão (IETF RFC 3261) é um padrão amplamente utilizado em comunicações VoIP para configurar e desativar chamadas SIP. A Figura 15 representa uma mensagem SIP que foi trocada durante a realização do teste.

Figura 15 – Mensagem SIP trocada.

Fonte: Autoria própria.

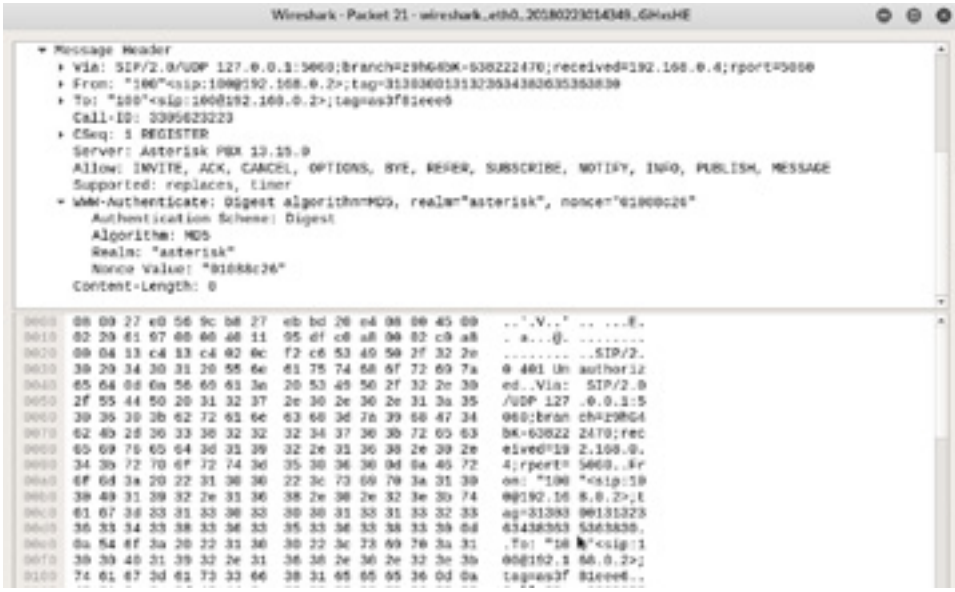
O dispositivo do usuário (chamado de *User Agent* na terminologia SIP) é registrado no servidor de registros responsável por manter um banco de dados de registros de todos os assinantes. No caso deste teste foi utilizado o Asterisk para servidor de registro e servidor proxy.

O registro do usuário no VoIP é necessário porque fornece os meios para lo-

calizar e contactar uma parte remota. Para um usuário se registrar, é feita uma solicitação utilizando um pacote SIP chamado REGISTER para o servidor de registro. Esse pacote carrega informações como nome de usuário, domínio ou IP de origem, domínio ou IP de destino, tempo de expiração do registro e algumas outras informações padrões do pacote SIP.

Ao receber a solicitação, o servidor de registro responde para este usuário um pacote SIP chamado 401 Unauthorized. Esse pacote foi baseado na autenticação em HTTP utilizando Digest (WWW-Authenticate), conforme Figura 16.

Figura 16 – Resposta com informações do registro.



Fonte: Autoria própria.

A autenticação *Digest* é um esquema de desafio/resposta que substitui a autenticação básica. O servidor de registro, dentro do pacote SIP 401 Unauthorized, envia uma cadeia de caracteres dos dados aleatórios chamados nonce ao usuário como um desafio.

O usuário responde com um *hash* que inclui o nome de usuário, senha e nonce entre informações adicionais. A complexidade que apresenta este *exchange* e o *hash* de dados, ou seja, utilização de senhas mais fortes, torna mais difícil roubar e reutili-

zar as credenciais do usuário com esse esquema de autenticação.

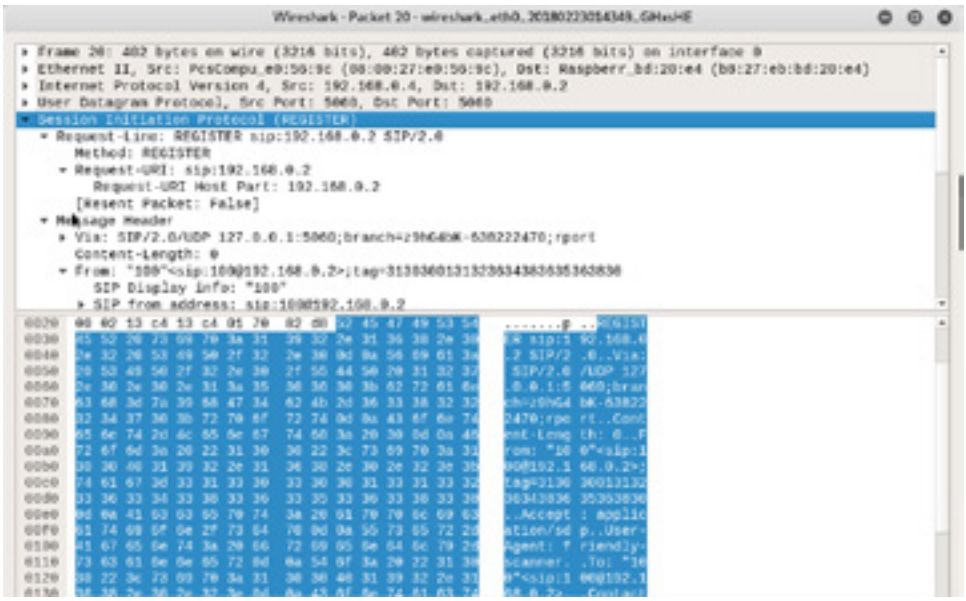
Quando o usuário quer entrar em contato com outro usuário, ele enviará uma solicitação INVITE para o servidor proxy. Servidores proxy são responsáveis em rotear mensagens SIP e localizar assinantes.

Quando o servidor proxy recebe uma solicitação INVITE, ele tenta localizar a parte chamada para retransmitir o progresso ao chamador executando várias etapas, como pesquisas de DNS e o roteamento de diversas mensagens SIP (provisórias e informativas).

Uma das mensagens roteadas para chegar até o usuário destino é a mensagem SIP 401 Unauthorized, o usuário só irá conseguir contactar o outro usuário quando responder o desafio com a *hash* correta. Com estes parâmetros, o invasor pode criar algorítimos de descoberta e quebra dessa cadeia de caracteres enviada pelo servidor de registro.

Entre algumas das aplicações utilizadas, está o ataque bruto que usa John The Ripper, dicionário ataque ou Quebrando a Resposta Digest. Utilizando o John the ripper, pode-se quebrar a senha e autenticar a extensão. A utilização de uma quebra de senha é um processo demorado e geralmente utiliza força bruta.

Figura 17 – Envio de pacote de REGISTER.



Fonte: Autoria própria.

No nosso experimento com o ataque de Autenticação, conforme cenário Figura 10, obti- vemos exito tendo em vista nenhuma implementação de segurança dentro ou fora do Raspberry Pi 3, também não identificamos nenhum problema junto ao *Software* Asterisk.

5.2 Ataque Man-in-the-middle

Espionagem em VoIP é um pouco diferente da escuta tradicional em redes de dados, mas o conceito geral permanece o mesmo. Escutas em VoIP exigem a interceptação da sinalização e dos fluxos de mídia associados de uma conversa. As mensagens de sinalização usam protocolos de rede separados (por exemplo, UDP ou TCP) e portas da própria mídia. Os fluxos de mídia geralmente são transportados por UDP usando o protocolo RTP (Real Time Protocol).

O ataque do tipo ARP-Spoofing ou envenenamento ARP é o meio mais eficiente de executar o ataque conhecido por Man-In-The-Middle e obter informações e fluxos de mídia em uma ligação VoIP. O *Address Resolution Protocol* (ARP) é um protocolo para mapear um endereço IP do endereço de uma máquina física (MAC) que é reconhecida na rede local.

Por exemplo, um IP versão 4 (IPv4), o tipo de IP mais comumente usado hoje em dia, tem 32 *bits* de tamanho. Em uma rede local Ethernet, entretanto, os endereços de dispositivos conectados possuem 48 *bits* de tamanho. Para aumentar a eficiência da rede e não engargalar a conexão realizando o broadcast do ARP, cada computador mantém uma tabela de endereços IP e endereços Ethernet na memória. Isto é chamado de cache ARP. Antes de enviar um broadcast para toda a rede, o computa- dor transmissor verificará se a informação existe em seu cache ARP. Se existir, ele completará os dados Ethernet sem enviar um broadcast ARP, evitando de engargalar a conexão. Cada entrada dura normalmente 20 minutos (mas depende do sistema operacional).

A RFC 1122 especifica que é possível configurar o valor do tempo de expiração do cache ARP no host. Para examinar o cache em um computador com Windows, UNIX ou Linux, digite “arp -a”no console ou prompt de comando. O ARP provê as regras do protocolo realizando esta correlação e possibilitando a conversão de endereços em ambas as direções.

5.2.1 Como a tabela ARP funciona?

Quando um pacote destinado a uma máquina de uma rede local particular chega no *gateway*, o *gateway* solicita ao programa ARP que encontre um host físico ou endereço MAC que esteja de acordo com o endereço IP. O programa ARP olha no ARP cache e, se encontra o endereço, retorna o mesmo e assim o pacote pode ser convertido ao formato e tamanho corretos, sendo enviado à máquina, Se nenhuma entrada é encontrada para o endereço IP, o ARP faz um broadcast de um pacote de requisição especial a todas as máquinas na rede para ver se uma das máquinas sabe qual delas tem o IP associado.

Se uma máquina reconhecer o endereço IP como o seu, ela retorna uma resposta indicando o fato. Assim, o ARP atualiza seu cache para futura referência e então envia o pacote de dados para o endereço MAC que respondeu. O ARP Spoofing é um tipo de ataque no qual uma falsa resposta ARP é enviada a uma requisição ARP original. Enviando uma resposta falsa, o roteador pode ser convencido a enviar dados destinados ao computador 1 para o computador 2, e o computador por último redireciona os dados para o computador 1. Se o envenenamento ocorrer, o computador 1 não tem ideia do redirecionamento das informações.

A atualização do cache do computador alvo (computador 1) com uma entrada falsa é chamado de envenenamento. Uma terceira pessoa está inserida entre o caminho de comunicação dos dois. Não há qualquer interrupção do tráfego de ambos os computadores, pois a terceira pessoa redireciona os pacotes de dados ao computador destino.

5.2.2 Realizando o Ataque

O Monitoramento de tráfego de VoIP pode permitir que um invasor capture pedidos SIP, dados RTP, captura de autenticação SIP e escutas de telefonemas. Para este ataque, o invasor utiliza o ataque chamado Man-in-the-middle (homem no meio) que exigem os seguintes passos:

- Envenenamento ARP / spoofing (arpspoof);
- sniffing tráfego (wireshark).

Comandos utilizado no kali linux para fazer o man in the middle:

Ativar o forward

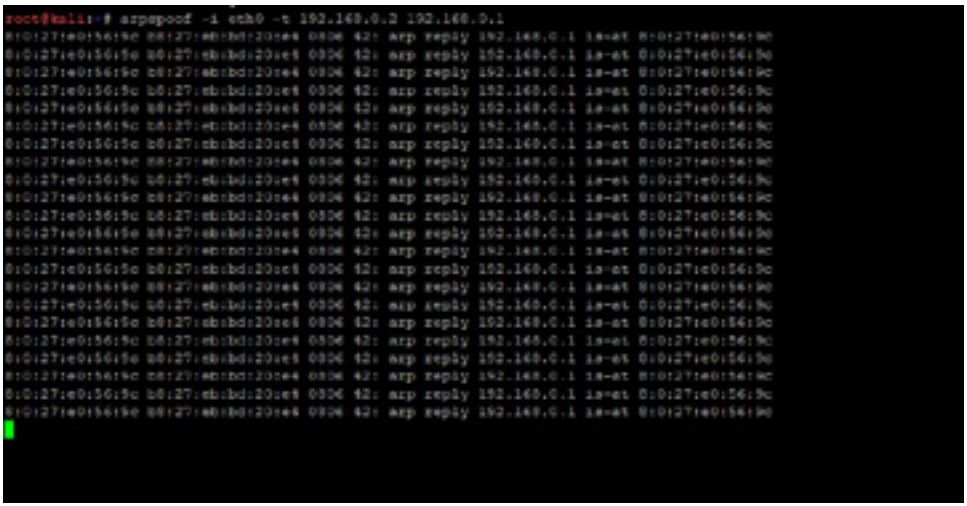
```
# echo “1? >  /proc/sys/net/ipv4/ip_forward

ou

# sysctl -w net.ipv4.ip_forward=1
```

Envenenar a tabela arp

```
# arpspoof -i eth0 -t 192.168.0.2 192.168.0.1
```

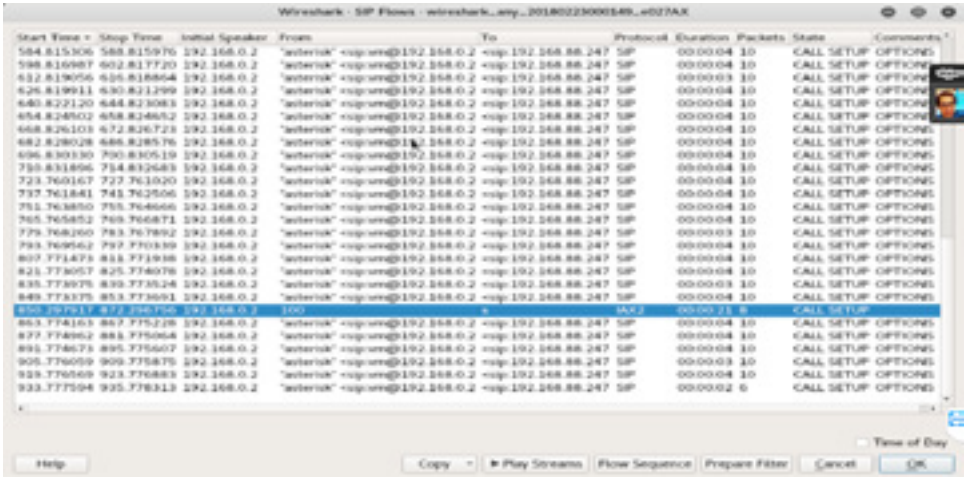
Na Figura 18 temos o resultado do comando que realiza o envenenamento da tabela ARP e com o Wireshark no kali linux o atacante consegue capturar os pacotes com a extensão 100, conforme a Figura 19.

Figura 18 – Ativação do arpspoof.



Fonte: Autoria própria.

Figura 19 – Captura de pacotes com wireshark.



Fonte: Autoria própria.

No experimento com o ataque de Ataque Man-in-the-middle, conforme Figura 18, obtivemos êxito, tendo em vista que não houve nenhuma implementação de segurança dentro ou fora do Raspberry Pi 3. Também não identificamos nenhum problema junto ao *Software* Asterisk.

5.3 Ataque Negação de Serviço DoS

O objetivo de qualquer ataque DoS é sobrecarregar o sistema com tantas solicitações ao ponto de ele ser forçado a encerrar. Os ataques DoS de telefonia são uma subcategoria em que esses tipos de ataques são nivelados em sistemas VoIP. Infelizmente, este tipo de ataque saltou para a frente das preocupações nos boletins de segurança como resultado de seu uso contra hospitais e linhas telefônicas 9-1-1.

Em outro desenvolvimento deprimente, alguns atacantes DoS exigem um resgate para deter o ataque. Muito parecido com o ransomware, com a ajuda de criptomoedas e spoofing de identificador de chamadas, é incrivelmente difícil identificar os invasores.

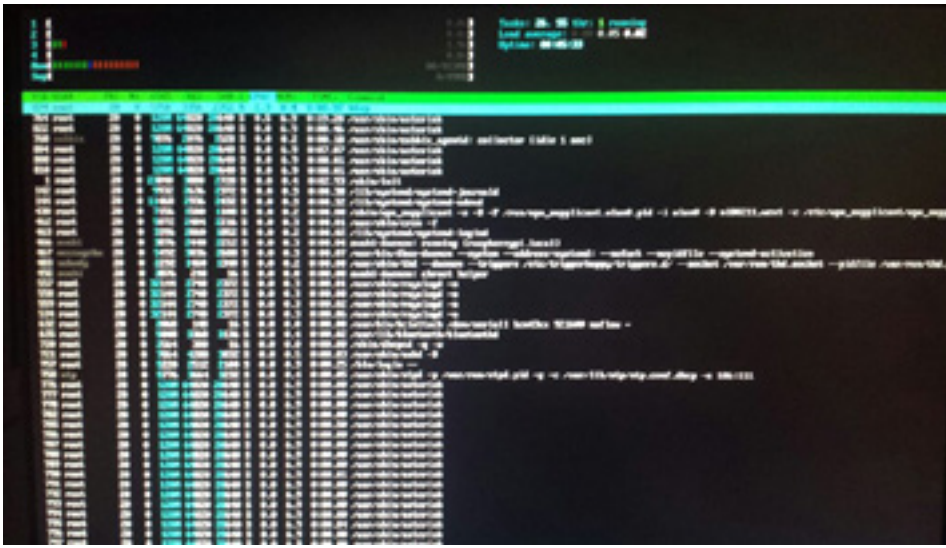
Os ataques TDoS geralmente empregam menos recursos do que os ataques DoS projeta- dos para prejudicar os sistemas de TI, como redes, servidores e software.

Em sua forma mais básica, tudo o que um ataque TDoS exige é um discador

telefônico automatizado que chame um número de telefone de destino e desligue – repetidamente. Esse conceito muito simples pode impedir qualquer outra pessoa de passar pela linha.

Com este ataque, o invasor inunda o aplicativo VoIP com inúmeras requisições e dados, o que pode levar ao travamento do PBX, impossibilitando o tráfego na rede. A Figura 20 nos mostra o estado do Raspberry Pi 3 antes do ataque, apresentando uma livre utilização de recursos, as 4 CPU's livres e utilizando 92 MB de memória RAM.

Figura 20 – Estado do Raspberry Pi 3 antes do ataque.



Fonte: Autoria própria.

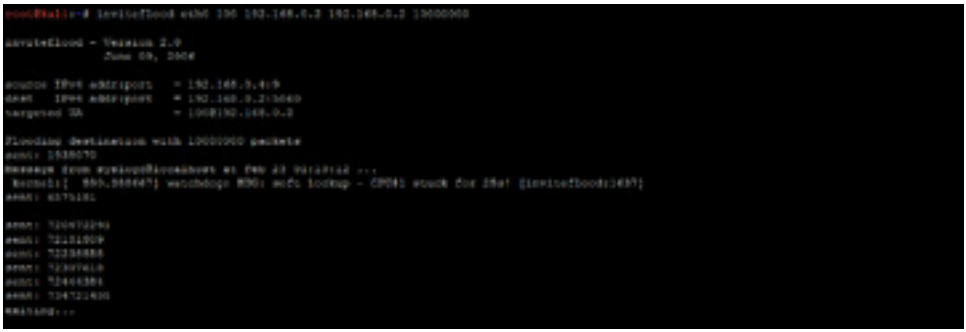
Primeiramente, vamos utilizar o kali linux para fazer o ataque de negação de serviço, conforme é demonstrado na Figura 21.

```
# inviteflood eth0 100 192.168.0.2 192.168.0.2 100000
```

Neste comando, temos o seguinte:

inviteflood : comando
eth0 : placa do usuário
100 : usuário
192.168.0.2: IP do PABX
192.168.0.2: IP doPABX
100000 : QuantidadePacotes

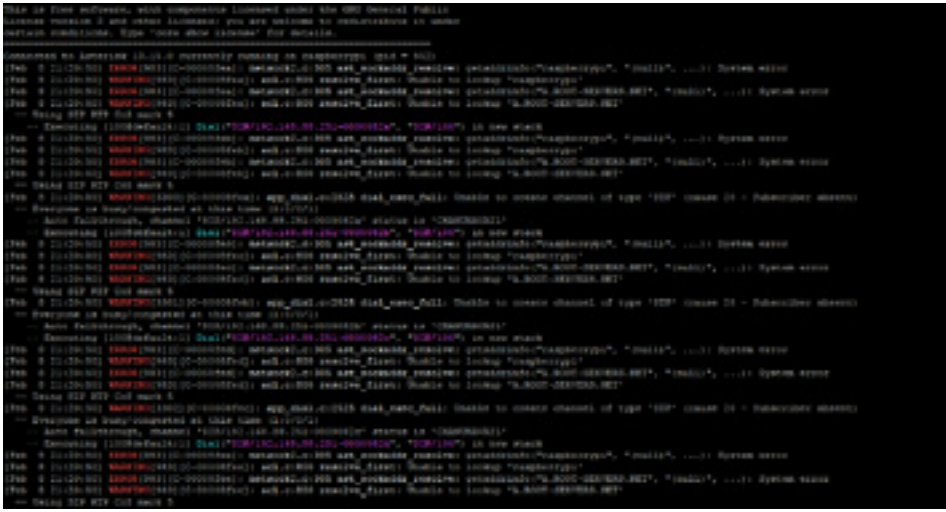
Figura 21 – comando inviteflood.



Fonte: Autoria própria.

No Asterisk do Raspberry Pi 3, o mesmo recebe os pacotes do atacante e começa a afetar a comunicação das linhas telefônicas ligadas ao Asterisk Figura 22. O Raspberry Pi 3, mesmo com um número grande de pacotes, ainda continua rodando, mas o *software* Asterisk, à medida que vai aumentado a quantidade de pacotes, começa a ser afetado.

Figura 22 – Resultado do ataque de DoS.



Fonte: Autoria própria.

No ataque de Negação De Serviço, que tem como característica o envio de pacotes, realizamos vários ataques com diferentes quantitativos de pacotes - conforme Tabela 3 para verificar o comportamento do Raspberry Pi 3 e do *software* Asterisk.

Tabela 3 – Análise de Ataque DoS por quantidade de pacotes.

Quant De Pacotes	Status Raspberry Pi	Status Asterisk	Status Da Chamada
00000	Excelente	Excelente	Sem Falha
10.000	Excelente	Excelente	Sem Falha
50.000	Excelente	Excelente	Sem Falha
75.000	Excelente	Excelente	Com falhas
100.000	Excelente	Excelente	Com falhas
250.000	Excelente	Bom	Com falhas
500.000	Excelente	Ruim	Com Muitas falhas
1.000.000	Excelente	Não funciona	Não funciona

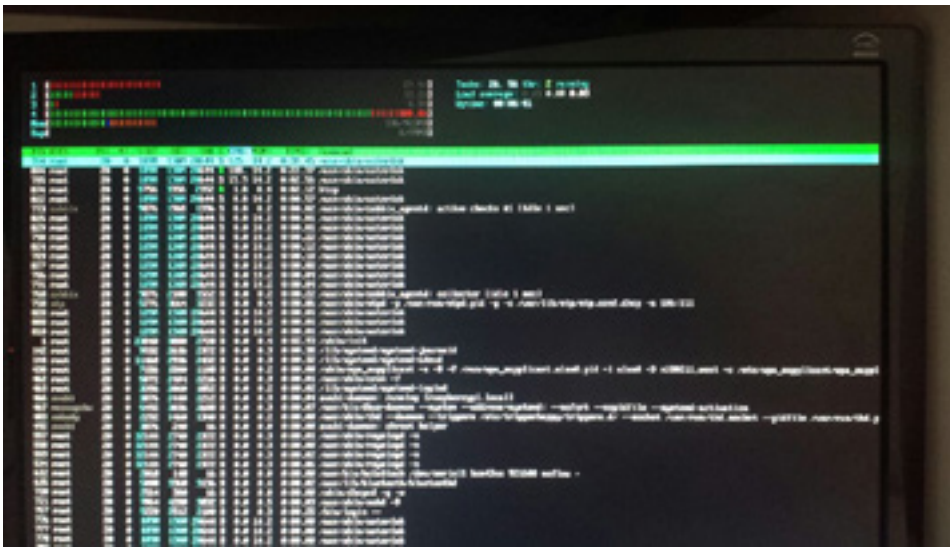
1.000.000	Ótimo	Não funciona	Não funciona
4.000.000	Ótimo	Não funciona	Não funciona

Fonte: Autoria própria.

Na realização do ataque de negação de Serviço, conseguimos monitorar o resultado do ataque no Raspberry Pi 3 com o Asterisk com a quantidade 1.000.000 pacotes. Foi obtido o resultado de uso de 100 por cento de uma das cpu´s e de toda a memória RAM conforme a Figura 23. Mesmo assim o Raspberry Pi 3 continuou funcionando normalmente. À medida que fomos aumentando a quantidade de pacotes, o funcionamento do Raspberry Pi 3 continuou mostrando ser muito bom.

O Asterisk começou a apresentar problemas a partir de 150.000 pacotes, tendo como consequência falha nas ligações, e a partir de 250.000 pacotes já ficava impossível entender as ligações, ultrapassando essa quantidade de pacotes o Asterisk já não funcionava. O Raspberry Pi 3 se mostrou muito eficiente até a quantidade de 4.000.000 de pacotes até onde realizamos o experimento.

Figura 23 – Uso da Memória e CPU.

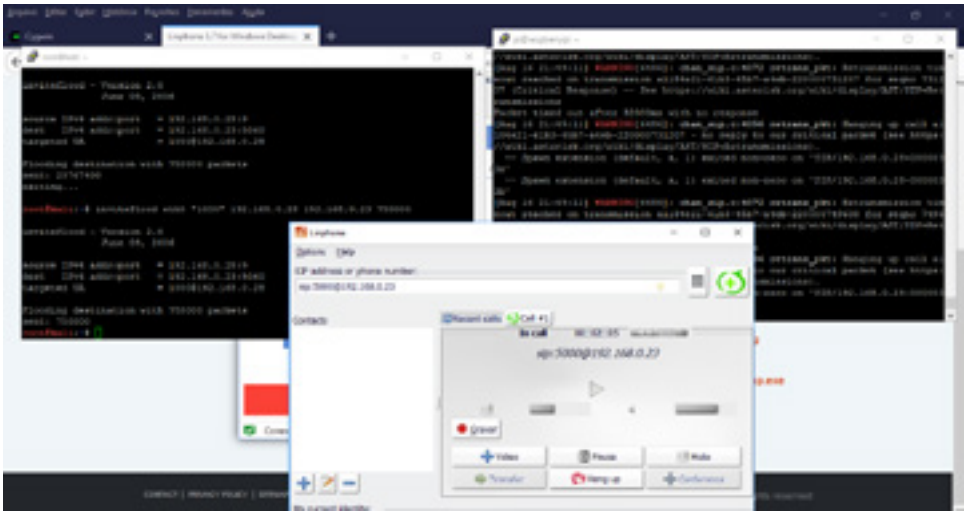


Fonte: Autoria própria.

5.4 Eficiência do processador e Memória nos ataques usando o Zabbix

Nesta seção, vamos mostrar o consumo do processador e da memória na realização dos ataques no Raspberry Pi 3 com o Asterisk em funcionamento com realizações de chamada conforme a Figura 24 . O Raspberry Pi 3, possui um total de 1GB RAM e um processador Broadcom BCM2837 de 64 *bits* e *clock* de 1.2GHz.

Figura 24 – Cenário para coleta de eficiência do Processador e Memória

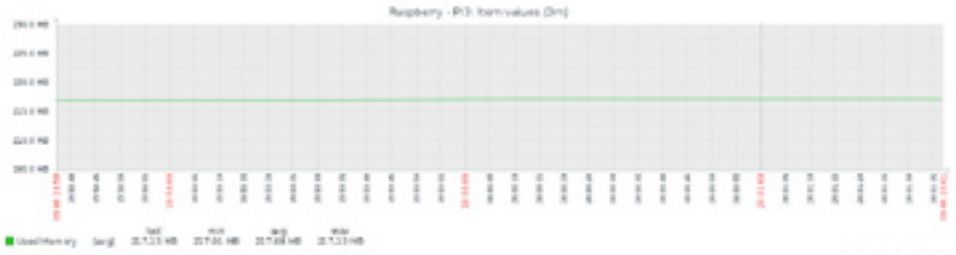


Fonte: Autoria própria.

Neste cenário, conforme Figura 24, utilizamos o Linphone para realizar chamadas durante os ataques juntamente com a maquina virtual para gerar o ataques no Raspberry Pi 3 com o Asterisk. As Figura 25 e Figura 26 no horário 19:58:00 até 20:00p:00, mostram a CPU e a memória antes de qualquer ataque.

No Ataque de Autenticação que estava sendo realizado exatamente às 20:00:10 e no Ataque Man-in-the-middle que ocorreu exatamente no horário de 20:01:00, não foi possível perceber alteração na memória nem no processador de modo a prejudicar o Raspberry Pi 3. No Asterisk também não houve perda em nenhum momento conforme Figura 25 e Figura 26. Como consequência, as ligações continuaram normalmente.

Figura 25 – Eficiência da Memoria



Fonte: Autoria própria.

Figura 26 – Eficiência do Processador

Fonte: Autoria própria.

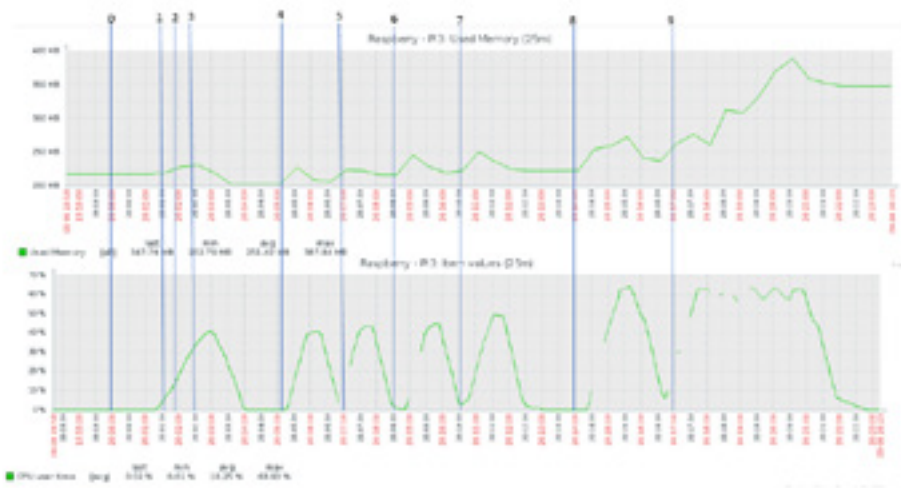
No Ataque Negação de Serviço DoS, realizamos a coleta das informações conforme Tabela 3 para que pudéssemos observar o que acontece em cada quantidade de pacote enviados ao Raspberry Pi 3 com Asterisk.

Na figura Figura 27, podemos observar a evolução do ataque de negação de serviço a começar pelo ponto “0”, Figura 27, este sendo o ponto em que o Raspberry Pi 3 com AsterisK ainda não sofreu ataque de negação de Serviço DoS ou seja não foi enviada nenhuma quantidade de pacotes, o que nos mostra que a memoria se encontra entre 200 MB e 250 MB e a CPU entre O e 5 % não demonstrando nem modificação no Raspberry Pi 3, AsterisK e nem problemas nas ligações.

Nos pontos 1 (10.000 pacotes), 2 (50.000 pacotes) e 3 (75.000 pacotes), podemos observar que a memória começa a subir com tendência a chegar ao ponto de 250 MB e a CPU sai de 0% a 40%. Mesmo com essa subida, nem Raspberry Pi 3 com AsterisK são afetados e continuam com seu funcionamento sem nenhuma alteração e as ligações continuam sem nenhum problema.

No ponto 4 (100.000 pacotes), podemos observar que a memoria fica entre os “O MB “e 225 MB descendo sua velocidade aos poucos. Já a CPU chega a ter o seu uso em 40 % e permanecendo com os mesmos por alguns ms (milésimos de segundos) conforme a Figura 27. Com essa quantidade de pacotes também não foi percebida nenhuma alteração no Raspberry Pi 3, AsterisK e nenhum problema nas ligações.

Figura 27 – consumo de Memoria e CPU em Ataque DoS



Fonte: Autoria própria.

No ponto 5 (150.000 pacotes, podemos observar que a memoria fica entre “O MB “e 225 MB descendo sua velocidade aos poucos. Já a CPU chega a ultrapassar o uso de 40 % e permanece com os mesmos por alguns ms (milésimos de segundos) conforme a Figura 27.

Com essa quantidade de pacotes, também não foi percebida nenhuma alteração no Raspberry Pi 3, mas no AsterisK as ligações começaram a ter interferências dificultando a escuta nos contatos provenientes dessa quantidade de pacotes. Perceba que na CPU - Figura 27 existe uma quebra na linha mostrando claramente o momento da dificuldade de transmissão.

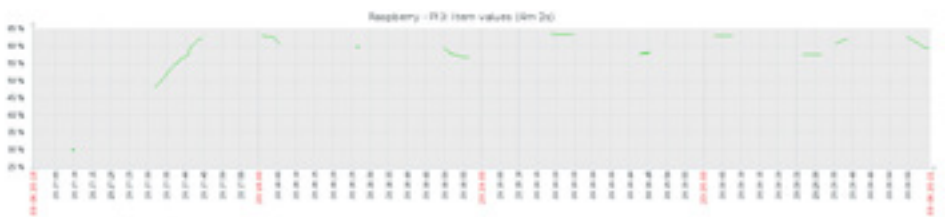
No ponto 6 (250.000 pacotes), foi observado que a memória fica entre “OMB“ e chega muito próximo de 225 MB, descendo sua velocidade aos poucos. Já a CPU

chega a ultrapassar o uso de 40 % e permanece com os mesmos por alguns ms (milésimos de segundos) conforme a Figura 27.

Com essa quantidade de pacotes, também não foi percebida nenhuma alteração no Rasp- berry Pi 3, mas no AsterisK foi observado que as ligações começaram a ter muitas interferências, dificultando profundamente a escuta proveniente da quantidade de pacotes. Note que na CPU, Figura 27 existe uma quebra na linha mostrando claramente o momento da dificuldade de transmissão.

Nos pontos 7 (500.000 pacotes), 8 (1.000.000 pacotes) e 9 (4.000.000 pacotes), houve uso da memoria entre 250 MB a próximo de 400 MB, mostrando a força do ataque de negação de serviço DoS. Já a CPU fica oscilando entre 0 % e 65 % aproximadamente. No ponto 7 e 8 houve uma perda de performance no Raspberry Pi 3. No AsterisK, foi observado que o sistema parou. Consequentemente, as ligações e os ramais foram desligados em decorrência da quantidade de pacotes. Podemos perceber mais claramente na Figura 28 que existem várias quebras de linha ao serem enviados 4.000.000 de pacotes ao Raspberry Pi 3 com Asterisk.

Figura 28 – 4.000.000 pacotes em CPU em Ataque DoS



Fonte: Autoria própria.

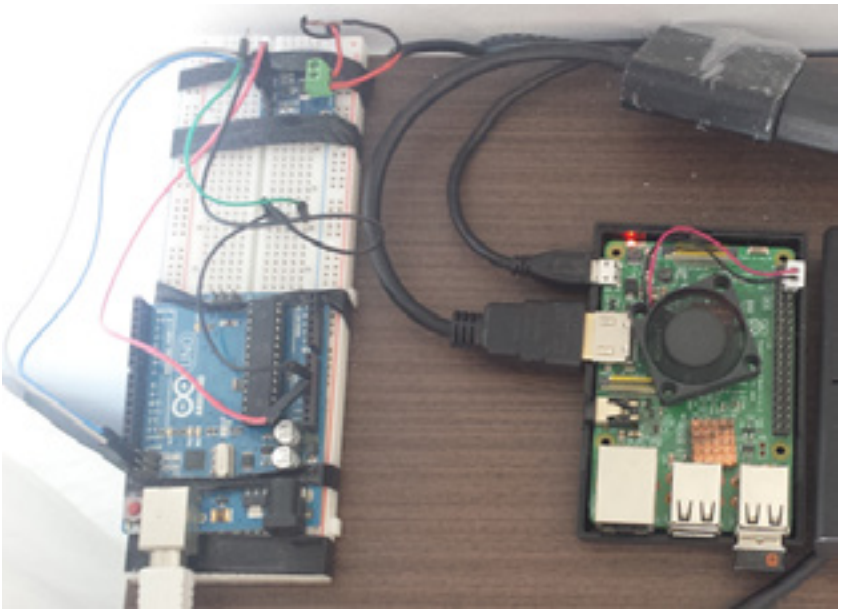
5.5 Consumo de Energia nos ataques usando Zabbix

O objetivo deste experimento é realizar uma análise de eficiência energética através da medição de corrente e de tensão elétrica no dispositivo embarcado Raspberry Pi 3 com Asterisk no momento de ligações com os ataques de Autenticação, ataque Man-in-the-middle e ataque de negação de serviço DoS.

Para isso utilizou-se um protótipo abordado por Maia (2017), o qual realiza uma medição física. O mesmo é constituído por um dispositivo embarcado Arduino Uno, que realiza a comunicação com a placa de monitoramento de tensão e corrente Ada-

fruit. Essa, por outro lado, utiliza um sensor de corrente e tensão INA219, desenvolvido pela empresa Texas Instruments conforme Figura 29.

Figura 29 – Dispositivo embarcado Arduino Uno com Raspberry Pi 3 com Asterisk.



Fonte: Autoria própria.

A Tabela 4 mostra a coleta da eficiência energética antes de qualquer ataque no Raspberry Pi 3 com Asterisk.

Tabela 4 – Coleta da eficiência energética inicial.

Estado Inicial de Energia		
Voltage (V) Média	Current (mA) Média	Power (mW) Média
5,21	-600,93	-3132,40
Desvio Padrao		
0,01	5,67	29,08

Fonte: Autoria própria.

No Ataque de Autenticação e no Ataque Man-in-the-middle, não foi percebido um consumo muito diferenciado do estado normal do Raspberry Pi 3 com Asterisk. A Tabela 5 mostra que não houve nada significativo que comprometesse o o funcionamento do Raspberry Pi 3 com o Asterisk.

Tabela 5 – Coleta de eficiência energética nos Ataques de Autenticação e Man-in- themiddle

Estado de Energia Ataque de Autenticaçao e Man-in-the-middle		
Voltage (V) Média	Current (mA) Média	Power (mW) Média
5,22	-558,29	-2916,22
Desvio Padrao		
0,00	5,84	30,68

Fonte: Autoria própria.

Na Figura 30 fica bem evidente que não existe uma diferença significativa entre o estado inicial e os ataques Ataque de Autenticação e no Ataque Man-in-the-middle.

Figura 30 – coleta de eficiência energética inicial x coleta de eficiência energética Ataque de Autenticação e no Ataque Man-in-the-middle.

Fonte: Autoria própria.

No Ataque Negação de Serviço DoS, utilizamos a medição pela quantidade de pacotes enviados para o Raspberry Pi 3 com Asterisk conforme Tabela 6 e Figura 31.

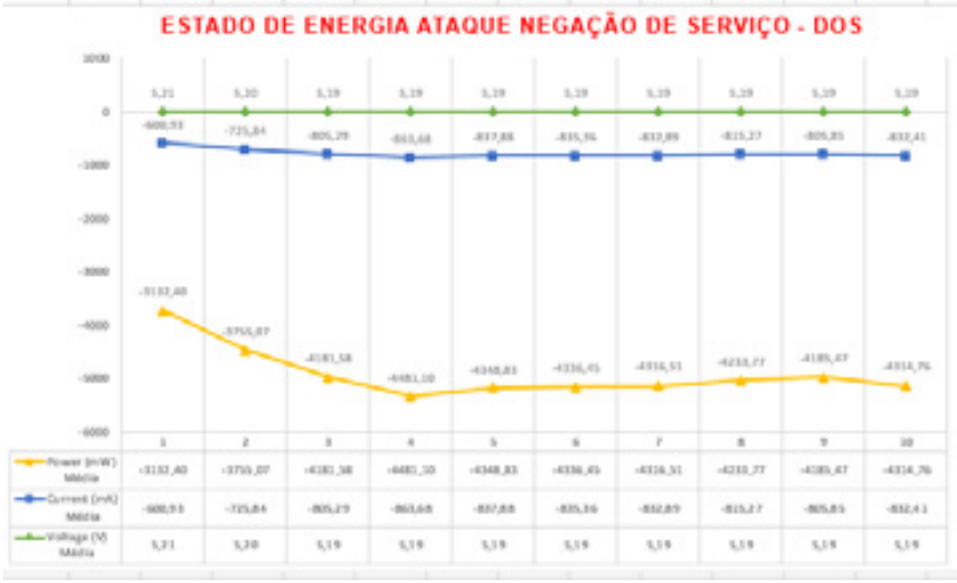
No ataque de negação serviço, podemos observar que quanto mais pacotes são enviados para o Raspberry Pi 3 com Asterisk a voltagem tende a ficar em um único patamar e a current e o power, a variar.

Tabela 6 – Coleta da eficiência energética no Ataque de Negação de Serviço - DoS.

Estado de Energia Ataque Negaçao de Serviços DoS			
Quant Pacotes	Voltage (V) Média	Current (mA) Média	Power (mW) Média
0	5,19	-600,93	-3132,40
10.000	5,19	-725,84	-3755,07
50.000	5,19	-805,29	-4181,58
100.000	5,19	-863,68	-4481,10
500.000	5,19	-837,88	-4348,83
750.000	5,19	-835,36	-4336,45
1.000.000	5,19	-832,89	-4316,51
1.500.000	5,19	-815,27	-4233,77
10.000.000	5,19	-805,85	-4185,47
25.000.000	5,19	-832,41	-4314,76

Fonte: Autoria própria.

Figura 31 – Eficiência energética no Ataque de Negação de Serviço - DoS.



Fonte: Autoria própria.

6
Conclusão

A segurança em Sistemas Embarcados nem sempre foi levada em conta uma vez que, inicialmente, a maioria deles operavam embutidos em sistemas sem conectividade exterior, como a internet. No entanto novas aplicações que utilizam o conceito de Sistemas Embarcados são dispositivos que precisam se interconectarem à Web via protocolos Internet e diversas conexões sem fio como WiFi, 3G/GPRS e mesmo a Ethernet com fio.

Conforme foi visto neste livro, as vulnerabilidades e ameaças estão por toda a parte, presentes em todos os elementos de infraestrutura que compõem a arquitetura VoIP. Seja um *hardware,* um *software*, um protocolo de comunicação ou mesmo os próprios usuários, todos esses elementos possuem vulnerabilidade que pode ser explorada. Um usuário desatento que acaba fornecendo informações para um invasor, seja um equipamento mal configurado ou sem atualizações, seja falta de conhecimento sobre os riscos dos protocolos e tecnologias utilizados para a implementação do VoIP, todas essas variáveis influenciam na segurança e privacidade das redes VoIP. Aliado ao fato de que aplicações para Sistemas Embarcados são geralmente desenvolvidas em C. A opção por está, se dar por sua eficiência, ou seja, aplicações escritas em C são usualmente mais rápidas e com isso mais adequadas a sistemas com pouco recursos como Sistemas Embarcados. Apesar disso, tal eficiência tem preço. Quando comparada a outras linguagens de programação, C não implementa alguns mecanismos de segurança, o que deixa suas aplicações mais vulneráveis que as demais. Desta forma neste livro, foi realizada uma abordagem de segurança em VoIP usando Asterisk e protocolo SIP em Plataforma Embarcada e uma análise de desempenho e eficiência energética no dispositivo embarcado Raspberry Pi 3 com Asterisk.

Nos Ataque de Autenticação e no Ataque Man-in-the-middle, ficou claro que o Raspberry Pi 3 com Asterisk não faz nenhuma interferência de funcionamento tanto no sistema embarcado como no Asterisk. Já no Ataque de Negação de serviço DoS, o Raspberry Pi 3 se mostrou muito eficiente no ataque, não mostrando perda em seu

desempenho nas quantidades de pacotes enviados neste trabalho.

Conforme Tabela 6 e Figura 31, o Asterisk por sua vez demonstrou que a quantidade de pacotes enviados para o Raspberry Pi 3 influencia no sistema ao ponto de parar todas as chamadas simultâneas, inviabilizando o uso do Raspberry Pi 3 com Asterisk.

Com relação ao consumo de energia nota-se que o Raspberry Pi 3 em sua voltagem tende a ficar em um patamar médio de 5,19v e a Current variando entre -600,93mA a -832,41mA e o Power variando entre -3132,40mV a -4314,78mV tendo com parâmetro a quantidade de pacotes enviados pelo atacante de 0 a 25.000.000. Raspberry Pi 3 com Asterisk mostra que o dispositivo é muito eficiente, mas o Asterisk não. Sendo assim existe a necessidade do dispositivo ter um sistema de segurança embutido que venha a garantir a segurança no Raspberry Pi 3 com Asterisk. Isso pode prejudicar o desempenho, tendo em vista que vai necessitar do uso de mais memória e processador.

Referências

AKYILDIZ, I. et al. Wireless sensor networks: a survey. *Computer Networks*, v. 38, n. 4, p. 393–422, 2002. ISSN 13891286. Disponível em: <http://www.sciencedirect.com/science/article/ pii/S1389128601003024>. Citado na página 13.

ALHAZMI, O. H.; MALAIYA, Y. K.; RAY, I. Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers and Security*, v. 26, n. 3, p. 219–228, 2007. ISSN 01674048. Citado na página 14.

BALL, S. R. *Embedded Microprocessor Systems: Real World Design*. 3. ed. EUA: [s.n.], 2005. 1–28 p. ISSN <null>. ISBN 9780750675345. Disponível em: <http://www.sciencedirect.com/science/article/pii/B9780750675345500230>. Citado na página 21.

BANSAL, A.; PAIS, A. R. Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System. In: *2015 IEEE International Conference on Computational Intelligence & Communication Technology*. IEEE, 2015. p. 391–396. ISBN 978-1-4799-6023-1. Disponível em: <http://ieeexplore.ieee.org/document/7078732/>. Citado 2 vezes nas páginas 35 e 36.

BARBOSA, C. S. VoWLAN : Voz sobre IP em Redes Locais Sem Fio. *Network*, Centro Federal de Educação Tecnológica de Goias, Goiânia, n. Ii, p. 1–17, 2006. Citado na página 25.

BARR, M.; REILLY, P. O. *Programming Embedded Systems in C and C++*. [S.l.: s.n.], 1999. 1–187 p. ISBN 1565923545. Citado 2 vezes nas páginas 14 e 15.

Brito S. H. B. *Aspectos de Segurança e Sigilo em Comunicações VoIP*. São Paulo: [s.n.], 2011. 13 p. Citado 2 vezes nas páginas 27 e 30.

BUTCHER, D.; LI, X.; GUO, J. Security challenge and defense in VoIP infrastructures. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, v. 37, n. 6, p. 1152–1162, 2007. ISSN 10946977. Citado na página 29.

CARRO, L.; WAGNER, F. R. Sistemas Computacionais Embarcados. *XXII Jornadas de Atua-*

lização em Informática - JAI, p. Capítulo 2, 2003. Citado 2 vezes nas páginas 14 e 15.

CHASE, O. Sistemas Embarcados. *SBAJovem 2010*, p. 7, 2007. Citado na página 22.

ČÍŽ, P. et al. VoIP Intrusion Detection System with Snort. *ELMAR, 2012 Proceedings*, n. September, p. 137–140, 2012. ISSN 13342630. Citado 2 vezes nas páginas 34 e 36.

COLHER, S. et al. *VoIP: Voz sobre IP*. 3. ed. Rio de Janeiro: [s.n.], 2005. 288 p. ISBN 9788535217878. Citado na página 13.

CUERVO, F. et al. *Megaco Protocol Version 1.0 RFC 3015 (Proposed Standrd). Obsoleted by RFC 3525.* [S.l.: s.n.], 2000. Citado na página 25.

CUNHA, A. Sistemas Embarcados. *Revista Saber Eletrônica 414*, Revista Saber Eletrônica 414, 2007. Citado na página 21.

Dalle Vacche, A.; Kewan Lee, S. *Zabbix Network Monitoring Essentials*. Birmingham: [s.n.], 2015. 178 p. ISBN 978-1784399764. Citado na página 31.

DASTERISK. *Definição de asterisk*. 2016. Disponível em: <http://www.asterisk.org>. Acesso em: 23 maio 2018. Citado na página 23.

DEFSIP. *Definindo o que é um protocolo de sinalização*. 2006. 01 p. Disponível em: <https://www.gta.ufrj.br/grad/06{_}1/sip/Definindooqueumprotocolodesinalizao.h>. Acesso em: 20 dez 2017. Citado na página 25.

GRECCO, F. Revista de TI. p. http://www.timaster.com.br/revista/artigos/main_ar, 2004. Disponível em: <http://www.timaster.com.br/revista/artigos/main{_}artigo.asp?codigo=>. Citado na página 20.

GROSS, F. D. *VoIP com Asterisk*. 1. ed. São PauloSão Paulo: Linux New Media do Brasil Editora Ltda. Coleção Academy, 2011. Citado 3 vezes nas páginas 24, 25 e 29.

HAMACHER, C. et al. *Computer Organization and Embedded Systems*. 6. ed. [S.l.]: Mc Graw-Hill, 2012. ISBN 978-0073380650. Citado na página 15.

HERTZOG;, R.; O'GORMAN;, J.; AHARONI, M. Kali Linux Revealed Mastering the PenetrationTesting Distribution. *European Journal of Organic Chemistry*, v. 2012,

n. 14, p. 2756–2765, may 2012. Disponível em: <http://doi.wiley.com/10.1002/ejoc.201200111>. Citado 2 vezes nas páginas 30 e 31.

International Telecommunications Union. Specifications of Signalling System No. 7. v. 1, 1993. Citado na página 20.

JONES, J. R. Estimating software vulnerabilities. *IEEE Security and Privacy*, v. 5, n. 4, p. 28–32, 2007. ISSN 15407993. Citado na página 14.

KELLER, A. Asterisk na prática. v. 2, p. 336, 2011. Citado 2 vezes nas páginas 19 e 25.

KUHN, D. R.; WALSH, T. J.; FRIES, S. Security Considerations for Voice Over IP Systems Recommendations of the National Institute of Standards and Technology Voice Over IP Systems. *Nist Special Publication*, 2005. Citado na página 13.

LOMOTEY, R. K.; DETERS, R. Intrusion Prevention in Asterisk-Based Telephony System. In: *2014 IEEE International Conference on Mobile Services*. IEEE, 2014. p. 116–123. ISBN 978-1-4799-5060-7. Disponível em: <http://ieeexplore.ieee.org/document/6924302/>. Citado 2 vezes nas páginas 33 e 36.

MAIA, W. P. *PROJETO, IMPLEMENTAÇÃO E DESEMPENHO DOS ALGORITMOS CRIPTOGRÁFICOS AES, PRESENT E CLEFIA EM FPGA*. Aracaju: Universidade Federal de Sergipe, 2017. Disponível em: <https://ri.ufs.br/bitstream/riufs/5029/1/WILLIAM{_}PEDROSA{_}MA>. Citado na página 54.

MARWEDEL, P. *Embedded System Design*. [s.n.], 2011. 258 p. ISBN 9780387300870. Disponível em: <http://books.google.com.br/books?id=DZEoizXV1swC>. Citado na página 15.

MCGRAW, G. *Software security: building security in*. [S.l.]: Addison-Wesley Professional., 2006. Citado na página 14.

MINOLI, D. *Delivering Voice Over IP Networks*. 2. ed. Indiana: [s.n.], 2002. Citado na página 26.

NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de rede em ambientes corporativos*. [S.l.]: Novatec, 2007. 482 p. ISBN 9788575221365 8575221361. Citado na página 26.

RAAKE, A. *Speech quality of VoIP: assessment and prediction*. [S.l.: s.n.], 2006. 336 p. ISBN 978-0-470-03060-8. Citado na página 18.

RAFAEL SEIDI SHIGUEOKA. *ANÁLISE COMPARATIVA DE TÉCNICAS PARA OCULTAMENTO DE PERDAS DE PACOTES EM APLICAÇÕES DO TIPO VOZ SOBRE IP (VOIP)*. 40 p. Tese (Doutorado) — Universidade Estadual de Londrina, 2016. Disponível em:<http://www.uel.br/cce/dc/wp-content/uploads/VersaoPreliminarTCC-Rafael-Shigueoka.pdf>. Citado na página 19.

REHMAN, U. U.; ABBASI, A. G. Security analysis of VoIP architecture for identifying SIP vulnerabilities. In: *2014 International Conference on Emerging Technologies (ICET)*. Islamabad, Pakistan: IEEE, 2014. p. 87–93. ISBN 978-1-4799-6089-7. Disponível em: <http://ieeexplore.ieee.org/document/7021022/>. Citado 2 vezes nas páginas 34 e 36.

REIS, C. *Sistemas Operacionais para Sistemas Embarcados"*. [S.l.]: ED-UFBA; BRASIL, 2004. Citado na página 21.

SINNREICH, H. *Internet communications using SIP: Delivering VoIP and multimedia services with session*. Indianapolis: Wiley Publishing, 2006. Citado na página 26.

SIQUEIRA, F. T. et al. Desenvolvimento de Sistemas Embarcados para Aplicacões Críticas. 2006. Citado na página 22.

SITOLINO, C. L. *Voz sobre IP – Um estudo experimental*. 1999. http://www.inf.ufrgs.br/pos/SemanaAcademica/Semana p. Disponível em: <http://www.inf.ufrgs.br/pos/SemanaAcademica/Semana99/sitolino/sitolino.html>. Acesso em: 16 ago 2018. Citado na página 13.

STAPKO, T. *Practical Embedded Security: Building Secure Resource-Constrained Systems*. [S.l.]: Embedded technology series. Elsevier Science., 2011. Citado na página 14.

TANENBAUM, A. S. *Redes de Computadores*. Rio de Janeiro: [s.n.], 2003. 946 p. ISBN 8535211853. Citado na página 21.

THERMOS, P. *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures*.

boston. [S.l.]: Pearson Education, Inc., 2007. ISBN 978-0321437341. Citado 3 vezes nas páginas 27, 28 e 29.

THERMOS, P.; ARI, T. *VOIP Network: Theats, Vulnerabilities and Countermeasures*. Boston, MA, USA: [s.n.], 2008. Citado 2 vezes nas páginas 27 e 28.

VOLCATEC. *VOLCATEC*. 2016. http://www.vocaltec.com p. Disponível em: <http://www.vocaltec.com>. Acesso em: 13 jul 2017. Citado na página 18.

WALKER, J. Q.; HICKS, J. T. *Taking Charge of Your VoIP Project*. 1. ed. [S.l.: s.n.], 2004. 312 p. ISBN 10: 1-58720-092-9. Citado na página 18.

WILLIAM; STALLINGS. *Criptografia e Segurança de redes, PRINCIPIOS E PRÁTICAS*. 6. ed. [S.l.]: Pearson Education, Inc., 2015. 557 p. ISBN 9788543014500. Citado na página 14.

YOSHIOKA, S. *Aspectos de Segurança para Telefonia IP utilizando o Protocolo SIP*. Campinas: UNICAMP, 2003. 73 p. Citado na página 30.

ZAPALS. *Raspberry Pi 3 Model B Motherbo- ard*. 2018. Disponível em: <https://www.zapals.com/raspberry-pi-3-model-b-motherboard-on-board-wi-fi-bluetooth-development-board-rs-original-uk-version. html>. Acesso em: 18 jan. 2018. Citado na página 23.