Proposta para Grupo de Trabalho Fase 2 – Ciclo 2021-2022

GT-Arquimedes: Uma Ferramenta para se Esquivar de Vazamentos de Informação na Transmissão de Mensagens de Rede (Fase 2)

Michele Nogueira Lima

26 de Setembro de 2021

1. Título

GT-Arquimedes: Uma Ferramenta para se Esquivar de Vazamentos de Informação na Transmissão de Mensagens de Rede

2. Coordenador Geral

Michele Nogueira Lima, Universidade Federal de Minas Gerais (UFMG)

Lattes: http://lattes.cnpq.br/7862253799240671

E-mail: michele@dcc.ufmg.br

3. Assistente de Inovação

WAGNER APARECIDO MONTEVERDE - EarlySec – Segurança Cibernética

LinkedIn: https://www.linkedin.com/in/wagnermonteverde

Email: wagner.ap.monteverde@gmail.com

Telefone: +55 44 9 9953 9690

4. Resumo

Este projeto desde sua concepção atua na prevenção de vazamentos de dados, uma necessidade cada vez maior diante das sanções da LGPD e a popularização da IoT. Particularmente, a equipe deste projeto atua em identificar vulnerabilidades de segurança a partir do tráfego da rede e em ofuscar o tráfego a fim de esconder essas vulnerabilidades. A identificação de vulnerabilidades, como tráfego não criptografado, segue métodos estatísticos, como entropia, e algoritmos de aprendizado de máquina. A ofuscação de vulnerabilidades parte da geração de tráfego falso em um primeiro momento. Essas duas funcionalidades compõem a ferramenta ARQUIMEDES que nesta fase 2 focaremos em oferecê-la como uma API a ser integrada em outras ferramentas e complementá-las. A ferramenta possui ainda um painel de controle.

5. Abstract

This project works to prevent data leaks, a growing need in the face of LGPD sanctions, and the popularization of the IoT. Particularly, this project focuses on identifying security vulnerabilities from network traffic and obfuscate the traffic to hide these vulnerabilities. Identifying vulnerabilities, such as unencrypted traffic, follows machine learning algorithms and statistical methods, such as entropy. The obfuscation of vulnerabilities comes from generating fake traffic in the first place. These two features make up the ARQUIMEDES tool, which in this phase 2 we will focus on offering it as an API to be integrated with other security tools and complementing them.
The tool also includes a dashboad to assist in the graphical visualization of the results.

6. Parcerias e respectivas contrapartidas

Universidade Federal de Minhas Gerais (UFMG) – a equipe na UFMG, instituição proponente desta proposta, é composta pela Profa. Dra. Michele Nogueira Lima (coordenadora da proposta) e o doutorando Nelson Prates, voluntário neste projeto, autor da dissertação de mestrado que deu origem à fase 1 do GT-ARQUIMEDES. A contrapartida da universidade consiste na infraestrutura e ambiente físico para desenvolvimento e testes da ferramenta, colocando a disposição equipamentos IoT para testes.

Universidade Federal do Paraná (UFPR) – a professora proponente foi transferida para a UFMG durante a fase 1 deste projeto, grande parte da fase 1 foi desenvolvida graças a infraestrutura da Universidade e alunos de mestrado e doutorado matriculados nesta. Uma parte da equipe (aluno de mestrado da professora) ainda está na UFPR e

utliza a infraestrtura da UFPR para trabalho e testes. A contrapartida da universidade consiste na infraestrutura e ambiente físico para desenvolvimento e testes da ferramenta, colocando a disposição equipamentos existentes no laboratório.

Universidade Federal de Santa Maria (UFSM) - Campus Frederico Westphalen – equipe complementar à da UFMG composta pelo Prof. Dr. Ricardo Macedo. Esta equipe auxiliará na gestão do projeto, no avanço de desenvolvimento da ferramenta proposta e na implantação da ferramenta na plataforma NasNuvens da RNP.

Start-up EarlySec – na liderança de Wagner Monteverde, a start-up irá auxiliar na construção e acompanhamento do modelo de negócio e transferência tecnológica.

7. Descrição da evolução do MVP com destaque para a entrada no NasNuvens da RNP

Na fase 2 deste GT serão realizadas melhorias no MVP visando a sua entrada no NasNuvens. As seguintes subseções descrevem em detalhes estas melhorias. Inicialmente será abordado o modelo de negócio, passando pela evolução da visão de negócio e do produto, o detalhamento dos clientes e usuários, quais pontos do MVP serão aprimorados e por fim quais as validações previstas.

7.1 Modelo de Negócio

O modelo de negócio segue uma abordagem de receita direta, onde a captura de receita ocorre por meio de uso direto da *Application Programming Interface* (API). Nesse modelo é cobrado dos consumidores um valor equivalente a um número de chamadas feitas, ou seja, pelo número de vezes que uma API é acessada para utilização dos serviços de análise, podendo ser um valor fixo ou não. Esse modelo é muito utilizado por empresas que oferecem serviços através de *Software as a Service* (SaaS).

Os principais modelos utilizados para receita direta via APIs são por meio do pagamento e do incentivo do uso da API. Quando envolve o pagamento, o valor a ser pago depende do consumo dos serviços de análise de dispositivos, sendo que os valores dependem da quantidade de dispositivos analisados. Quanto maior a quantidade de dispositivos menor é o preço pago por dispositivo, obedecendo faixas de consumo previamente definidas.

Além disso, um modelo de incentivo de utilização da API também é empregado. Neste caso, o usuário recebe um limite grátis para utilização do serviço e verifica a necessidade de analisar sua infra completa, nos moldes anteriores. Por exemplo, pode ser atribuído um limite grátis de X dispositivos identificados a partir do tráfego da rede a serem analisados. O valor X precisa ser analisado e validado, o que ocorrerá ao longo da fase 2 em caso de aprovação desta proposta. Cabe salientar que este segundo modelo desempenha um papel fundamental para a prospecção de clientes, uma vez que os mesmos passam a conhecer os benefícios da API sem ter um custo para passar a conhecer a importância da sua utilização em um determinado ambiente ou infraestrutura.

7.2 Evolução da Visão de Negócio e a Visão de Produto

A visão de negócios e a visão de produto evoluíram durante a execução da Fase 1 aos objetivos da Fase 2. Esta evolução pode ser observada considerando o segmento de clientes, a proposta de valor e as fontes de receita. Durante a primeira fase, a equipe do GT-Arquimedes passou por processos de pivotagem destes pontos. Inicialmente, os segmentos de clientes foram organizados em dois grandes grupos, considerando nesses segmentos os clientes do sistema RNP, como a Rede Universitária de Medicina. Na nossa classificação, o primeiro grupo possui preocupações imediatas em relação à presença de vulnerabilidades de segurança nas aplicações, serviços e dispositivos da IoT, tais como as empresas do setor da saúde e do setor automotivo. O segundo grupo seriam os clientes que neste momento ainda não visualizam essas vulnerabilidades como um risco ao seu negócio, como por exemplo, o setor de agronegócio, impulsionados pela implantação da tecnologia de comunicação 5G. Para a Fase 2, a equipe do GT-Arquimedes passou também a considerar as empresas prestadoras de serviços de segurança da informação como clientes com alto potencial, além de possíveis clientes no sistema RNP e a complementariedade da solução em serviços já oferecidos aos clientes do sistema RNP, como o serviço Eduroam.

A proposta de valor também evoluiu durante a condução da fase 1. Na fase 1, a proposta de valor foi elaborada com base no levantamento de hipóteses, aprimoradas por meio de três grandes reflexões. A primeira partia do princípio de que os clientes eventuais possuíam interesse na quantificação e eliminação do risco das vulnerabilidades de segurança capazes de comprometer a correta operação das infraestruturas digitais de seus eventuais clientes. A maior parte desta proposta de valor se manterá durante a fase 2, no entanto, foi definido um escopo no que tange a eliminação do risco das vulnerabilidades. Esta delimitação foi feita com base no emprego de uma técnica de ofuscação dos comportamentos dos dispositivos IoT, onde um tráfego é forjado para confundir eventuais análises do tráfego da rede desempenhadas por usuários mal intencionados. A proposta de ofuscação, em seu nível MVP no momento, precisa e será aprimorada na fase 2.

Por fim, as fontes de receita também foram revistas no decorrer da fase 1 do projeto. Foram idealizadas na fase 1 três fontes de receitas: mensalidades, implantação e consultorias. As mensalidades seriam implantadas em três formas, anuais, bianuais ou trianuais. Para a fase 2 foi considerada uma abordagem de receita direta, onde a captura de receita ocorre por meio de uso direto da API. Neste caso, a fonte de receita depende da quantidade de uso da API em análises e um limiar de uso gratuito passaria a ser usado para incentivar o uso da solução desenvolvida.

7.3 Clientes e Usuários

A ferramenta proposta possui um painel de controle e também possibilita a integração com diferentes sistemas de gestão da segurança da informação. Neste sentido, os clientes e usuários alvo da oferta inicial da solução contemplam tanto o Sistema RNP quanto o mercado em geral. A partir da perspectiva do Sistema RNP, podem ser considerados o *Computer Security Incident Response Team* (CSIRT), o Centro de Atendimento a Incidentes de Segurança (CAIS), os Pontos de Presença da RNP (PoPs) e um complemento ao serviço Eduroam. Os CSIRTs consistem em equipes responsáveis por receber, analisar e responder notificações e atividades maliciosas. Atualmente a RNP apoia 15 CSIRTs distribuídos entre diferentes estados brasileiros. O

CAIS acompanha todo o ciclo de tratamento de incidentes de segurança, compreendendo a etapa de monitoramento, detecção, triagem e resolução de atividades maliciosas. Os PoPs oferecem serviços avançados para prover conectividade à infraestrutura nacional de alto desempenho mantida pela RNP. Enquanto que o serviço Eduroam oferece um serviço federado para autenticação de usuários em redes Wi-Fi, permitindo que um usuário utilize as credenciais de acesso de sua instituição de origem para acessar redes sem fio de diferentes universidades, centros de pesquisa, praças, aeroportos e cafeterias. A API deste projeto pode expandir o serviço Eduroam de forma integrada ou não a este a fim de analisar as vulnerabilidades de segurança no tráfego de rede de acesso e até mesmo auxiliar na ofuscação dessas redes nas instituições.

Os clientes da API também podem pertencer ao mercado em geral, sem considerar o Sistema RNP. Neste caso, os eventuais clientes poderiam ser empresas da área de segurança de redes, as quais desenvolvem suas próprias ferramentas para analisar grandes quantidades de dados em busca de ameaças e vulnerabilidades em seus clientes. Para estes clientes, a solução desenvolvida agregará um nível de informação adicional em relação às ferramentas atualmente empregadas, uma vez que as características específicas dos dispositivos IoT serão consideradas, o que é um grande diferencial.

7.4 Melhorias no MVP

Para a Fase 2 do GT-Arquimedes, um conjunto de melhorias das funcionalidades já existentes no MVP estão previstas. Estas melhorias abordarão o processo de instalação no cliente, a captura do tráfego da rede, a identificação do tipo dos dispositivos IoT, a busca por vulnerabilidades, o procedimento de ofuscação e a separação do ARQUIMEDES da ferramenta Sherlock, desenvolvida previamente pela StartUp e que serviu de base no desenvolvimento do MVP da fase 1. Uma breve descrição de cada uma destas funcionalidades são descritas a seguir, bem como as diretrizes estipuladas para assegurar o seu aprimoramento.

O ***processo de instalação*** compreende a forma como o MVP será implantado na infraestrutura dos clientes para realizar a coleta do tráfego, análise de vulnerabilidades e ofuscação do comportamento dos dispositivos IoT. Durante a condução da primeira fase do projeto, esforços foram realizados para criar uma máquina virtual para facilitar este processo. Todavia, foram identificadas limitações nesta abordagem, uma vez que existe a dependência de uma infraestrutura computacional disponível no cliente para hospedar essa máquina virtual. Além disso, a implantação do MVP requer configurações especializadas na máquina virtual, envolvendo a configuração das interfaces de rede responsáveis por coletar o tráfego e por obter as informações necessárias para ajustar o procedimento de ofuscação do comportamento da rede. Durante a fase 2, a equipe do GT-Arquimedes pretende aprimorar estes procedimentos de instalação do MVP agregando um software na máquina virtual para realizar o procedimento de instalação no cliente de maneira interativa, onde o administrador de redes passa a informar as configurações especializadas da sua infraestrutura.

A ***captura do tráfego*** (sensor de coleta de tráfego) desempenha uma função chave no MVP para a realização das análises de vulnerabilidades em dispositivos IoT [1]. Na fase 1 do GT, esta captura foi realizada ao configurar um computador equipado com uma interface de rede sem fio para operar como um gateway. Desta forma, os dispositivos

IoT gerenciados necessitavam conectar na rede criada e as atividades de pré-processamento necessárias pela análise do tráfego da rede eram realizadas neste computador. Todavia, esta abordagem revelou limitações no momento da implantação do MVP em um *early adopter,* visto que de maneira geral os clientes já possuem um gateway previamente configurado e a sua substituição pode acarretar outros problemas técnicos, gerando transtornos em seu ambiente de produção. Para a fase 2, a equipe do GT-Arquimedes considerará duas possibilidades, sendo elas empregar o espelhamento do tráfego da rede e a adição de um equipamento físico para realizar a coleta. No primeiro caso, seriam exploradas soluções em nível de software para serem aplicadas possivelmente no firewall da rede de modo a filtrar e encaminhar o tráfego da rede. Enquanto que no segundo caso, será considerada a possibilidade de incluir um dispositivo com especificações mínimas de hardware e com uma configuração de interface de rede habilitada em modo promíscuo para realizar a captura dos tráfego com a mínima interferência na rede do cliente. Essas alternativas precisam ser analisadas e validadas antes de se decidir pela qual seguir de fato.

Aprimoramento na ***identificação do tipo do dispositivo*** IoT ocorre no MVP para agrupar equipamentos com as mesmas vulnerabilidades, sendo refletida diretamente na interface gráfica [2]. Este procedimento foi desenvolvido empregando algoritmos de aprendizagem de máquina tendo como entrada o tráfego da rede para posteriormente realizar o treinamento. No entanto, durante a fase de treinamento torna-se necessário obter um rótulo como informação base para permitir classificar com precisão as amostras que guiam o processo de descobrimento automático posteriormente realizado por meio da aprendizagem de máquina. Nos esforços iniciais do GT, este rótulo foi atribuído de maneira estática de modo a validar a proposta de valor do MVP como um todo. Ainda na fase 2 foram realizados esforços para empregar a ferramenta Nmap para obter tais rótulos de maneira automatizada para a fase de treinamento do algoritmo. Entretanto, a equipe não teve tempo hábil de implementar essa funcionalidade em sua totalidade. Portanto, durante a fase 2 do projeto serão empregados esforços para finalizar esta melhoria no MVP.

A **busca por vulnerabilidades** em uma rede IoT também consiste em uma funcionalidade de fundamental importância no MVP, uma vez que está diretamente relacionada com a proposta de valor. Cabe salientar a ausência de uma base de dados consolidada na literatura com vulnerabilidades específicas para dispositivos e rede IoT. Para guiar esta funcionalidade, o GT-Arquimedes segue as dez principais vulnerabilidades para dispositivos IoT elencados pela *Open Web Application Security Project* (OWASP) [3], sendo elas a transferência insegura de dados (7° posição OWASP), a presença de mecanismos inseguros (4° posição OWASP) e a ausência de proteção da privacidade (6° posição OWASP). No estágio atual, a transferência insegura de dados ocorre ao identificar tráfego de rede não emprega os protocolos *Transport Layer Security* (TLS) ou *Secure Sockets Layer* (SSL), bem como pelo emprego da entropia de Shannon nos pacotes do tráfego de rede para verificar se os mesmos estão criptografados ou não. A presença de mecanismos inseguros ocorre por meio da análise do tráfego da rede em busca de comunicações em portas conhecidas por oferecer serviços inseguros na rede, tal como o *File Transfer Protocol* (FTP) e o Telnet. Durante a fase 2, nossa intenção inicial era trabalhar na identificação de outras vulnerabilidades elencadas pela OWASP. Porém, diante de limitações orçamentárias, nos limitaremos a aperfeiçoar a indentificação das vulnerabilidades tratadas na fase 1.

A **ofuscação** do comportamento de dispositivos IoT atua no MVP como uma alternativa para contornar a condução de ataques cibernéticos sofisticados, onde o usuário malicioso emprega técnicas de inteligência artificial no tráfego de rede para violar o direito da privacidade dos usuários ao obter informações sobre o cotidiano dos usuários legítimos com base na utilização dos seus equipamentos IoT [4, 5, 6, 7]. Por meio da ofuscação, o MVP forja um tráfego de rede para simular a existência de outros dispositivos na rede ou para gerar indícios da utilização dos dispositivos reais em momentos nos quais de fato eles não estão operando. Como resultado do emprego da ofuscação, o atacante recebe informações incorretas do tráfego de rede de sua vítima, acarretando consequentemente em uma análise equivocada do comportamento dos usuários reais e da topologia da rede. No estado da arte este tipo de situação está sendo classificada como *Adversarial Deep Learning* [8, 9].

Durante a fase 1 do projeto, a equipe do GT-Arquimedes desenvolveu uma versão inicial da ofuscação, abordando a ofuscação por tipo de dispositivos e da rede como um todo. No entanto, durante a fase 2 serão desenvolvidas evoluções desta funcionalidade para estabelecer uma periodicidade da execução do procedimento, uma vez que atualmente ele é executado apenas quando o usuário discriminadamente aciona a funcionalidade na interface gráfica e depois nenhuma outra ação é executada. Da maneira como se encontra essa implementação, ela será efetiva apenas se o atacante está capturando o tráfego enquanto administrador aciona a função de ofuscação. Outra melhoria na ofuscação será a atualização da ferramenta de geração do tráfego da rede, pois na fase 1 foi empregada o *Scapy Traffic Generator* e a mesma foi descontinuada durante a execução da fase 1 do projeto e consequentemente não será adaptada para operar nas próximas versões dos sistemas operacionais [10], ocasionando o risco de tornar a funcionalidade de ofuscação obsoleta. Portanto, a equipe do GT-Arquimedes encontrará uma biblioteca ou ferramenta para substituir o *Scapy Traffic Generator*, bem como fará as adaptações necessárias para adaptar essa modificação no MVP como um todo.

Outro ponto a ser aprimorado na ofuscação durante a fase 2 do projeto consiste na investigação sobre a relação entre o aumento da privacidade e a quantidade de sobrecarga ocasionada com a geração de pacotes. Caso o procedimento de ofuscação resulte em uma quantidade intensa de tráfego em busca da garantia da privacidade dos usuários, o surgimento de degradações de desempenho pode ocorrer como um efeito colateral. Uma situação oposta, onde uma quantidade efêmera de tráfego de rede pode não assegurar o direito da privacidade dos usuários legítimos em situações de ataques cibernéticos sofisticados. Logo, durante a fase 2 do projeto, a equipe do GT-Arquimedes voltará seus esforços na busca de uma relação balanceada entre estes cenários.

A **separação** da ferramenta ARQUIMDES da ferramenta Sherlock. A fim de viabilizar o desenvolvimento do MVP na fase 1 e também com umsa visão de integrar o ARQUIMEDES na plataforma Sherlock-X da StartUp, algumas funcionalidades da ferramenta ARQUIMEDES foram herdadas como contrapartida da StartUp. Porém, com a evolução do modelo de negócio da plataforma ARQUIMEDES, vislumbra-se uma separação dessas duas ferramentas a fim de facilitar a comercialização e implantação.

Durante a fase 2, o MVP passará por modificações para permitir a sua **oferta na plataforma NasNuvens d**. A principal alteração do MVP consistirá na criação de funcionalidades para permitir a quantificação do uso da plataforma em análises, uma vez que o modelo de negócios será baseado em sistemas de API. A ideia deste modelo

de negócios surgiu no final da fase 1 do projeto e como consequência a versão atual do MVP ainda precisa ser modificada para suportar esse conceito.

7.5 Validações Previstas

Durante a fase 1 do projeto, a equipe do GT-Arquimedes identificou ao menos três alternativas em potencial para validar seu MVP. A primeira possibilidade consistiu na implantação da solução desenvolvida em uma loja de informática moderna, a qual emprega uma estratégia de marketing baseada em usar em sua própria infraestrutura os seus produtos mais modernos, tais como plataformas IoT para gerenciamento de lâmpadas e fechaduras inteligentes. Neste caso esta loja atuaria como *early adopter*, tendo a oportunidade de usufruir de um sistema moderno de gestão da segurança da informação para dispositivos IoT. Uma das vantagens em validar o MVP com este parceiro consiste na proximidade física com a Startup EarlySec, facilitando o processo de implantação e eventuais correções e adaptações para em um segundo momento partir para um ambiente maior e mais complexo.

As outras duas possibilidades de validação envolvem ambientes de emulação e uma parceria com a equipe do sistema Eduroam da RNP. Em termos de emulação, o GT-Arquimedes estudou durante a primeira fase a integração da ferramenta no ambiente IoT-Lab, um ambiente conhecido na literatura para testes com sensores e comunicação entre objetos IoT com características heterogêneas. Todavia, não existiu tempo hábil durante a fase 1 para garantir a implantação da solução neste ambiente. Durante a segunda fase essa possibilidade será reconsiderada.

Além disso, existe a possibilidade de validar o MVP juntamente com a equipe Eduroam em algumas instituições que utilizam o serviço como a UFMG e a UFSM. Esta possibilidade se mostra muito promissora devido ao grande número de dispositivos IoT que atualmente podem se conectar nesta infraestrutura. Ainda durante a fase 1 a equipe do GT-Arquimedes se reuniu com as lideranças do serviço Eduroam da RNP e um contato inicial foi estabelecido com o intermédio da RNP. Para a fase 2 a prevemos uma melhor interação com a equipe do serviço Eduroam para validar o MVP em um ambiente real e de larga escala.

8. Cronograma de marcos

E1 - Até 15/10/2021 - Especificação da Equipe: o GT submeterá a lista de forma completa os membros da equipe e seus dados pessoais, papéis e remuneração bruta atribuída. Junto ao relatório preenchido, deverá ser entregue a documentação para contratação de todos os bolsistas do projeto.

E2 - Até 29/10/2021 - Especificação da Infraestrutura: o GT deve entregar um relatório com o planejamento da infraestrutura que será requisitada para o desenvolvimento do projeto, considerando os limites orçamentários definidos

E3 - Até o último dia útil de cada mês - Relatórios Mensais de Atividades: o GT irá entregar um relatório mensal contendo uma breve descrição das atividades realizada por cada membro contratado da equipe.

E4 - Até 15/12/2021 - Plano de Desenvolvimento da Modelagem do Produto/Serviço: o grupo apresentará um plano para desenvolver a modelagem do produto/serviço, considerando os ajustes em relação ao MVP da fase 1, que deverá ser implementado ao longo da fase 2 do GT com o objetivo de divulgar a proposta de valor para segmentos de clientes, visando capturar interessados e validar o modelo com foco no Sistema RNP.

E5 - Até 31/01/2022 - Primeira Versão do Catálogo de Serviços do GT: uma primeira versão do catálogo de serviços a ser oferecido pelos resultados do GT será entregue para apreciação inicial da RNP. Neste catálogo, devem ficar claras as ofertas pagas e deve conter pelo menos uma oferta de degustação do produto/serviço sem custos. A oferta de degustação será foco de validação durante a fase 2 do GT.

E6 - Até 31/02/2022 - Atualização da Landing Page: o GT irá atualizar a landing page da solução desenvolvida no contexto do GT, com o intuito de capturar interesse de potenciais clientes.

E7 - Até 30/03/2022 - Minuta revisada do Acordo de Agência e Distribuição do NasNuvens: a startup EarlySec avaliará as condições comerciais de entrada na plataforma NasNuvens e entregará a minuta revisada do Acordo de Agência e Distribuição do NasNuvens. Este acordo prevê a possibilidade de cadastro da oferta na plataforma e a gestão desta oferta por parte da RNP. O acordo inicial prevê uma oferta para degustação sem custos para os usuários.

E8 - Até 31/05/2022 - Política de Segurança do Produto/Serviço para o Sistema RNP: o GT entregará uma política de segurança do produto/serviço para tratamento dos eventuais incidentes de segurança.

E9 - Até 30/06/2022 - Política de Privacidade do Produto/Serviço para o Sistema RNP: o GT entregará uma política de utilização e armazenamento dos dados pessoais do produto/serviço para atendimento da Lei Geral de Proteção de Dados (LGPD). Este documento deve descrever quais dados serão coletados dos usuários e como eles serão utilizados pela solução em desenvolvimento.

E10 - Até 30/06/2022 - Termos de Uso do Produto/Serviço para o Sistema RNP O GT entregará um documento descrevendo as condições de uso do produto/serviço para o Sistema RNP. Este documento descreve quais as condições comerciais para a utilização do produto/serviço resultado do GT.

E11 - Até 31/10/2022 - Relatório sobre a Validação do Modelo de Negócio do Produto/Serviço para o Sistema RNP: o grupo apresentará um relatório com os resultados e o processo realizados para a validação do modelo de negócios proposto pelo GT para a plataforma NasNuvens da RNP, explicitando as instituições e usuários que utilizaram a solução e/ou demonstraram interesse em utilizar a solução.

E12 - Até 30/11/2022 - Versão Final para o Catálogo de Serviço: entrega de uma versão atualizada do catálogo de serviços a ser oferecido pelos resultados do GT.

E13 - Até 15/12/2022 - Código-fonte e Documentação do Produto/Serviço para o Sistema RNP: ao final do projeto, o grupo deverá entregar a última versão do código-fonte desenvolvido no ambiente de desenvolvimento colaborativo da RNP e documentação técnica e manuais de uso e instalação/configuração da solução.

9. Recursos financeiros

9.1 Infraestrutura

A soma dos recursos solicitados não deve exceder R$ 25.000,00. Indicar subtotais nas tabelas abaixo.

9.1.1. Recursos de Nuvem

Usar como referência as informações sobre IaaS descritas no "Catálogo de equipamentos e Serviços de nuvem pública IaaS".

Categoria	Descrição da Configuração	Mês Inicial	Mês Final	Unid.	Qtd.	Custo Médio Unitário (R$)	Subtotal em R$ estimado
Servidor virtual	SERVIDOR VIRTUAL TIPO 1.4 vCPUs (4 vCPUs e, no mínimo, 14 GB de RAM, HD 50GB, 150 IOPs)	11/2021	12/2022	720hora /mês	14	R$ 1.192,00	R$ 16.688,00
Servidor virtual	SERVIDOR VIRTUAL TIPO 1 - 1 vCPU (1 vCPUs, 3,5 GB de RAM, HD 50GB, 150 IOPs)	12/2021	12/2022	720hora /mês	13	R$ 268,80	R$ 3.494,40
Servidor virtual	SERVIDOR VIRTUAL TIPO 2 2 vCPUs (2 vCPUs, 3,75 GB de RAM, HD 50GB, 150 IOPs)	12/2021	12/2022	720hora /mês	13	R$ 369,60	R$ 4.765,80
						Total	R$ 24.948,20

9.1.2. Referências

[1] Apthorpe, N., D. Reisman, and N. Feamster. "A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. arXiv 2017." arXiv preprint arXiv:1705.06805.

[2] Miettinen, Markus, et al. "IoT sentinel: Automated device-type identification for security enforcement in iot." 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2017.

[3] OWASP IoT Top 10. Disponível em: https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introdu ction-and-Root-Causes.pdf. Último acesso: 26 de Setembro de 2021.

[4] Prates, Nelson, et al. "A Defense Mechanism for Timing-based Side-Channel Attacks on IoT Traffic." *IEEE GLOBECOM* 2020.

[5] Prates, N. Um mecanismo de defesa contra ataques traffic side-channel temporais no contexto da IoT. Dissertação de Mestrado, UFPR, Curitiba, PR. 2020.

[6] Prates, N., Vergütz, A., Macedo, R. e Nogueira, M. Análise de vazamentos temporais side-channel no contexto da Internet das Coisas. Anais do XXIV Workshop de Gerência e Operação de Redes e Serviços (WGRS) no XXXVII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC), 24(3):157–170, 2019.

[7] Prates, N., Vergûtz, A., Macedo, R. e Nogueira, M.. Um mecanismo de defesa contra ataques traffic side-channel temporais na IoT. XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2019.

[8] Shi, Yi, et al. "Vulnerability detection and analysis in adversarial deep learning." Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham, 2018. 211-234. [9] Restuccia, F., D'Oro, S., Al-Shawabka, A., Rendon, B. C., Chowdhury, K., Ioannidis, S., & Melodia, T. (2020, July). Generalized wireless adversarial deep learning. In Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning (pp. 49-54).

[10] Goodbye Scapy, Hello snappi. Disponível em: https://opennetworking.org/wp-content/uploads/2021/05/2021-P4-WS-Chris-Sommers-Ankur-Sheth-Slides.pdf. Último acesso: 26 de Setembro de 2021.