Título do Trabalho

Internet das Tretas: como a Internet das Coisas afeta nossa segurança e privacidade?

Formato do workshop

Mesa redonda: motivada por perguntas orientadoras para estimular uma discussão entre os membros da mesa;

Proponente

Nome
Gustavo Paiva

Nome da entidade proponente
Centro de Articulação em Tecnologia e Sociedade (CATS.natal)

Setor
Comunidade científica e tecnológica

Co-Proponente

Nome
Sávyo Morais

Nome da entidade proponente
Universidade Federal do Rio de Janeiro (UFRJ)

Setor
Comunidade científica e tecnológica

Palestrante #1

Nome
Thiago Barçante Teixeira

Organização
ANATEL

Mini Biografia
Engenheiro Eletrônico e de Telecomunicações (PUC-MG), Especialização em Microeletrônica - Microfabricação de Circuitos Integrados (UFMG). Ocupa o cargo de Especialista em Regulação de Serviços Públicos de Telecomunicações, na Coordenação de Regulamentação Técnica da Gerência de Certificação e Numeração da Anatel.

Setor
Governamental

Palestrante #2

Nome
Emylle Varela

Organização
CATS.natal

Mini Biografia
Graduanda em Redes de Computadores, trabalha no setor de TI da Secretaria de Estado do Trabalho, da Habitação e da Assistência Social do RN. Teve seu primeiro contato com a GI como fellow no IGF 2015, desde então desempenha atividades de conscientização em torno do uso seguro, ético e responsável das TICs em escolas do RN como embaixadora SID. Hoje é membro do Youth Observatory e do CATS.natal.

Setor
Terceiro Setor

Palestrante #3

Nome
Sávyo Morais

Organização
UFRJ

Mini Biografia
Bacharel em Tecnologia da Informação pela UFRN (2017), Mestrando em Informática na UFRJ. Atualmente é membro do Universal Acceptance Steering Group da ICANN, onde vem publicando estudos desde 2018. Já participou de reuniões do IETF, IGF, ICANN, Lacnic e CGI.br, tendo sido bolsista dos programas de bolsas do Lacnic, Youth@FIB, NextGen@ICANN, ICANN Fellow e Youth Brasil promovido pelo CGI.br.

Setor
Comunidade Científicia e Tecnológica

Palestrante #4

Nome
Pollyanna Ringon

Organização
Loggi

Mini Biografia
Cientista da Computação pela URI - Campus Erechim-RS. Trabalhou por mais de 7 anos em ISPs, e hoje é DevOps na Loggi. Diretora Administrativa da ISOC Brasil, atuou em projetos de inclusão digital. Embaixatriz do Dia da Internet Segura pela Safernet Brasil, foi bolsista de programas Youth@FIB, Youth@IGF, ISOC LAC Taller e ICANN NextGen, e facilitadora no programa Youth Brasil 2020 do CGI.br.

Setor
Empresarial

Relatora

Nome
Ingrid Santos
Organização
UFAM

Mini Biografia

Graduanda em Ciência da Computação na Universidade Federal do Amazonas - (UFAM). Pesquisadora na área de Segurança de Sistemas Computacionais com ênfase em Privacidade. E integrante das comunidades Cunhantã Digital e Pyladies Manaus.

Setor
Comunidade Científicia e Tecnológica

Moderador

Nome
Claudio Miceli

Organização
UFRJ

Mini Biografia
Possui graduação em Ciência da Computação (2007), Mestrado em Informática (2010) e Doutorado em Informática (2014), todos pela Universidade Federal do Rio de Janeiro (UFRJ). Atualmente é professor da UFRJ, no Programa de Engenharia de Sistemas e Computação, atuando principalmente em Redes de sensores sem fio, Fusão de dados, Escalonamento, Cidades inteligentes e Computação em Nuvem.

Setor
Comunidade Científicia e Tecnológica

Objetivos e Resultados Propostos

Expor os pontos de vista dos diferentes stakeholders, de modo a permitir o entendimento dos seguintes pontos:

1. As ações do governo para garantir a segurança dos dispositivos IoT presentes no mercado;
2. Como a academia tem trabalhado para aprimorar as tecnologias presentes;
3. Os riscos aos quais os usuários finais estão expostos e suas preocupações;
4. Como a segurança tem afetado o processo de desenvolvimento dos dispositivos.

Além disso, também esperou-se como resultado um estreitamento de laços entre os órgãos reguladores nacionais e os demais atores para facilitar tanto o desenvolvimento de novas regulações, quanto a adequação às regulações atuais.

Objetivos e Resultados Atingidos

O workshop conseguiu atingir todos os seus objetivos propostos da seguinte maneira:

- Inicialmente foram apresentados os riscos e preocupações dos usuários finais quanto a segurança da IoT, ressaltando principalmente a necessidade de cuidado com o vigilantismo e a segurança física;
- Em seguida, foram apresentados os principais problemas de segurança enfrentados pelos ISPs nacionais, destacando-se principalmente a utilização de senhas fracas e senhas padrão, assim como configurações que geram fragilidade. Também foram elencados os cuidados tomados pelos desenvolvedores de *software* relacionados dispositivos IoT têm tomado para se prevenir dos riscos;
- A apresentação realizada pelo representante da Anatel -- Thiago Barçante -- esclareceu ao público quais as políticas estão sendo adotadas pelo governo federal para a homologação de dispositivos de Internet das Coisas a partir do ponto de vista da segurança cibernética.
- Por fim, foram apresentados os esforços realizados pela comunidade científica e tecnológica para reforçar a segurança do ecossistema da IoT a partir da adaptação de esquemas criptográficos e de autenticação, da detecção de incidentes e do

controle de acesso. Também levantou-se a necessidade de suporte das áreas de conhecimento humanísticas no entendimento de comportamentos padrão da sociedade sobre a tecnologia para o melhor desenvolvimento de soluções.

O estreitamento de laços entre o órgão regulamentador também aconteceu, trazendo ao conhecimento as chamadas públicas realizadas pelo governo, assim como apresentando outros meios de interação entre Anatel, sociedade civil e empresas interessadas.

Justificativa em relação à governança da Internet

A segurança de IoT vem sendo pauta de vários atores da Governança da Internet durante os últimos anos. O IETF, por exemplo, publicou em 2019 a RFC 8576 que elenca os desafios em estado-da-arte para a segurança de IoT. O documento discute problemas ligados à limitação da tecnologia enfrentados pela indústria, e o que isto acarreta para o usuário final.

Em um ambiente mais diverso, o IGF 2019 debateu, durante a seção “The Future of IoT: Toward More Secure and Human-Centered Devices”, que reuniu palestrantes da ISOC, Microsoft e instituições de governos e sociedade civil para debater o tema sobre os diversos pontos de vista.

Um dos atores mais ativos no combate à insegurança da IoT são operadores de TLDs, que têm desenvolvido pesquisa, lançando notas técnicas ou até soluções tecnológicas visando melhorar aspectos de segurança da IoT. Dois exemplos são o .nl e o .ca, da Holanda e Canadá, respectivamente, que desenvolveram seus próprios *firmwares* para roteadores domésticos que implementam barreiras de segurança para os dispositivos IoT a nível de rede.

ISPs também têm se preocupado com outras questões, como o consumo de banda por tráfegos de ataques DDoS, procurando alternativas para mitigar seus danos. Estes, porém, muitas vezes podem esbarrar em questões relacionadas à neutralidade da rede.

No cenário brasileiro, atores como o CERT.br têm publicados relatórios e artigos científicos relacionados a *botnets* compostas por dispositivos IoT. Já durante o VII Fórum da Internet no Brasil (2017) a Seção Plenária em Cibersegurança abordou o tema da segurança de IoT diluído dentro da discussão geral de cibersegurança. Além disso, em 2019 foi publicado o decreto nº 9.854, que institui o Plano Nacional de Internet das Coisas e, entre outras ações, insere regulação, segurança e privacidade, como temas fundamentais para o desenvolvimento da IoT no país.

Metodologia e formas de participação desenvolvidas durante o Workshop

Nos 5 minutos iniciais, o moderador passou para o público uma visão geral sobre o contexto de IoT, segurança e privacidade.
Em seguida, cada um dos 4 palestrantes teve 10 minutos para apresentar seu ponto de vista sobre o tema, respondendo a uma pergunta balizadora baseada em ao menos uma das seguintes linhas:

1. Quais são as dificuldades e riscos que você tem enfrentado?
2. O que você tem feito para enfrentar os problemas aos quais está exposto?
3. Que tipo de política você adota, ou acha que deve ser adotada neste enfrentamento?

Depois disto foi iniciada a sessão de interação de 30 minutos, onde perguntas realizadas pelo público através do YouTube foram direcionadas aos palestrantes.

Por fim, foram dados 15 minutos para considerações finais, encerrando a discussão da mesa.

Síntese dos debates

Tipo de Manifestação	Conteúdo	Consenso ou Dissenso	Pontos a Aprofundar
Posicionamento	Claudio Miceli (UFRJ): O Objetivo da mesa redonda é discutir sobre dispositivos de Internet das Coisas que coletam dados e tem se tornado cada vez mais comuns no ambiente doméstico, uma vez que podem se conectar a dispositivos que se comunicam com a internet. Contudo, também passam a ser pontos de vulnerabilidade e diante disso temos a necessidade de pensar no desenvolvimento seguro destes.	Consenso	Não Aplicável
Posicionamento	Emylle Varela (CATS.natal): Diante do seguinte questionamento “Quais são as principais preocupações dos usuários de IoT?” acreditava-se que a causa da baixa adesão da Internet das Coisas seria o preço alto dos produtos. Contudo, em estudo realizado por uma instituição no Brasil concluíram que 70% dos entrevistados consideravam os dispositivos inseguros e, portanto, tinham receio de fazer uso dos mesmos. Dessa forma, fica a reflexão quanto a importância de uma regulamentação e conscientização acerca da segurança de tais dispositivos. Buscando trazer uma visão da sociedade civil, foi produzido um vídeo utilizando de uma história lúdica sobre o uso de dispositivos IoT como forma de facilitar o dia-a-dia do usuário a fim de coletar a opinião dos entrevistados sobre o tema. Refletindo acerca dos comentários dos entrevistados no vídeo é notável que há pessoas que tenham receio do uso de maneira geral, outras fariam amplo uso da tecnologia, e alguns apresentaram preocupações quanto ao uso dos dados coletados pelos dispositivos. Diante disso, é perceptível a necessidade de se entender a sociedade civil e suas compreensões e necessidades de conscientização acerca do uso de tecnologias	Consenso	Não Aplicável

	de forma segura.		
Posicionamento	Pollyanna Rigon (Loggi): Diante do escopo de acesso à Internet no que diz respeito aos dispositivos inteligentes, temos que a Internet passa por vários pontos de conexão para que haja o envio de uma requisição e receba a resposta para a mesma. Os dispositivos inteligentes que temos em casa precisam de alguma forma para se comunicarem e de certo eles estarão conectados a um roteador que possui acesso a Internet. Aqui temos o primeiro ponto de reflexão, pois mesmo ainda que tenhamos a ideia de que o dispositivo esteja conectado apenas com o celular, ou com uma assistente virtual, na realidade temos que ele está exposto na Internet ainda que ele não necessite de acesso a rede para seu funcionamento. Assim, temos uma brecha para riscos de vazamentos de dados pessoais, empresariais, etc. Dito isso, o primeiro ponto a ser levantado diz respeito às configurações padrões que vem nos dispositivos, que acabam por ser brechas padrão nos dispositivos, uma vez que essas configurações estão disponíveis facilmente na internet e podem ser utilizadas para invadir dispositivos na qual o usuário não realizou a modificação. Portanto faz-se importante a prática da modificação dessas configurações para garantir um certo nível de segurança do usuário.	Consenso	Não Aplicável
Posicionamento	Thiago Barçante (Anatel): O que o governo, mais especificamente a Anatel, tem feito para abordar esse assunto da segurança cibernética em equipamentos para telecomunicação? Um dos princípios da Anatel para a avaliação da conformidade e homologação é a proteção dos usuários dos serviços para telecomunicações. O conceito de segurança nos equipamentos ganhou nova dimensão que é a segurança cibernética, e a Agência já tem tomado ações para, em breve, avaliar a segurança dos equipamentos para telecomunicações nesse novo paradigma. Neste ano de 2020, o Governo Federal publicou o decreto 10.222/20, que	Consenso	Não Aplicável

	estabelece a estratégia nacional de segurança cibernética, onde fica estabelecido que os órgãos da administração pública devem implementar ações que possibilitem a implantação das estratégias, e cada órgão deve atuar no âmbito de sua competência. Além disso, outro documento publicado também neste ano foi a instrução normativa nº4, do gabinete de segurança institucional da presidência da república que dispõe de requisitos mínimos de segurança que devem ser adotados no estabelecimento das redes de quinta geração. Ao tratar de segurança cibernética nos equipamentos em si é importante lembrar que os equipamentos para telecom possuem características técnicas bem diversificadas com relação a interface, processamento de memória etc. Além dessas características, temos a diversidade de suas aplicações, com isso a Anatel possui cerca de 217 classificações de produtos/tecnologias que necessitam de homologação. Devido a complexidade no processo de criação de regulamentações relacionados a segurança cibernética a agência publicou no início do ano uma consulta pública com recomendações de segurança cibernética que devem ser seguidas pelos fabricantes de produtos e, no momento, as contribuições estão sendo analisadas para melhorar o documento, de tal forma que, uma vez pronto, quando uma empresa for pedir a homologação do seu produto, ela terá de informar a quais requisitos o produto atende, e essa declaração estará pública de forma que o consumidor poderá consultar a quais requisitos o fabricante declarou que o produto atende. Em caso de verificação da não seguridade do produto, a Anatel poderá realizar a suspensão da homologação até que o fabricante realize as modificações necessárias, e a agência poderá até cancelar a homologação caso o fabricante não seja capaz de adequar o produto. De todo modo, estes documento ainda encontra-se em processo de construção com base nas contribuições públicas, mas são ações que a Anatel pretende implementar para abordar as questões de segurança cibernética.		
Posicionamento	<u>Sávyo Morais (Labnet/UFRJ):</u>	Consenso	Não

	É importante destacar o papel da Academia no trabalho de melhorar a proteção da IoT a partir de todas as áreas de conhecimento. As humanidades, como Ciências Sociais e Psicologia, ajudam a entender o padrão de comportamento dos usuários no contato com a IoT para entender quais as brechas de segurança que são criadas por eles, enquanto juristas auxiliam na criação de ferramentas jurídicas para proteger os usuários. Dentro da computação, os maiores esforços hoje estão em melhorar os esquemas criptográficos e de autenticação/autorização nos dispositivos para reduzir a possibilidade de intrusões e vazamentos de dados. A nível de rede, tem-se trabalhado em ferramentas de suporte à detecção de intrusão baseadas em inteligência artificial, assim como tem-se trabalhado também em mecanismos de controle de acesso de rede para os dispositivos para impedir a realização de atividades maliciosas por estes dispositivos. A comunidade tecnológica tem trabalhado em cima da RFC 8520 - Manufacturer Usage Description (MUD) -, que define meios para que um dispositivo IoT diga exatamente quais as comunicações de rede ele pode realizar, através de comunicação direta com o administrador da rede ao estabelecer conexão. Isto permite o bloqueio de tráfegos que não são esperados pelo dispositivo, reduzindo a possibilidade de infecção dele. A partir dos estudos sobre a MUD, tem-se desenvolvido o INXU - Intra Network eXposure analyzer Utility -, uma ferramenta que possibilita a especialista de segurança protegerem redes IoT domésticas de ataques conhecidos, sem quebrar a privacidade. A combinação da MUD com o INXU possibilita ter uma lista de bloqueios em cima da lista de permissões que acaba por reduzir o funcionamento de ataques. Em experimentos de laboratório realizados com o INXU, foi possível reduzir em 100% o funcionamento da *botnet* Mirai.		Aplicável
Proposta	<u>Pergunta:</u> Com a pandemia, o acesso ao mundo digital foi ampliado bastante (aulas remotas, compras em sites, acesso a serviços variados e trabalho corporativo). Quais	Consenso	Não Aplicável

	medidas devemos adotar tendo em vista que o mundo todo está conectado? Emylle Varela: O cuidado que se deve ter com a IoT não difere muito do que já se deve ter com outros dispositivos cibernéticos. É importante atentar para as especificações de segurança dos dispositivos, utilizar senhas fortes, utilizar sistemas atualizados e recomendados pelo fabricante, utilizar sistemas de criptografia para proteção dos dados, e tentar se atualizar sobre o surgimento de vulnerabilidades do produto. Também recomenda-se a separação dos dispositivos de uso geral e os de IoT em redes distintas para evitar a proliferação de ataques dentro da própria rede.		
Proposta	Pergunta: A Internet das coisas é uma realidade, certo? Não há como voltar atrás. O que o usuário comum, com pouco conhecimento técnico pode se proteger? Pollyana Ringon: O usuário final sempre pode questionar e cobrar ações do ISP contratado ou de algum outro especialista. Também é importante ressaltar a necessidade de ações éticas e proativas por parte da comunidade técnica em esforçar-se mais ao desenvolver uma solução ou configurar um serviço para o usuário final. Sávyo Morais: Outra coisa que é importante de se ter em mente é o entendimento de que a rede evolui. Isto quer dizer que uma senha fraca configurada hoje para a rede Wi-Fi da sua casa pode permitir que seu vizinho acesse as imagens de uma câmera de segurança que você comprar daqui 2 anos. Então a preocupação com a segurança deve ser constante. Claudio Miceli: Além de tudo isso, também é notável que, quando uma tecnologia nova é lançada, a comunidade técnica como um todo ainda leva um tempo para entender quais as fragilidades trazidas por esta tecnologia.	Consenso	Não Aplicável
Posicionamento	Pergunta:	Consenso	Não

	Caso a ANATEL homologue algum produto devesse ser barrado, existe algum canal próprio para enviar uma crítica ou sugestão de correção? Thiago Barçante: Além das recomendações feitas pela ANATEL para a segurança cibernética dos equipamentos de IoT, também estão definidas recomendações para os fabricantes e distribuidores dos dispositivos disponibilizarem meios para que usuários finais e/ou academia possam comunicar falhas de segurança encontradas. Além disso, a ANATEL disponibiliza canais de comunicação para que sejam feitas denúncias e reclamações sobre os dispositivos, o que pode levar à suspensão da certificação e da comercialização do equipamento caso a falha seja comprovada, só podendo ter as vendas retomadas quando a falha for resolvida.		Aplicável
Posicionamento	Pergunta: A utilização da MUD e do INXU não afetaria ainda mais a privacidade do usuário final? Sávyo Morais: Na verdade, a preservação da privacidade é uma das principais premissas no desenvolvimento do INXU. A maneira como os ataques são descritos permite que a proteção seja realizada mesmo que não se tenha acesso aos dados internos da rede, o que inclui informações da MUD, já que as informações de ataques vêm de maneira anonimizada para a rede interna, e apenas dentro dela é que é realizado o cruzamento destas informações de ataques com os dados da rede interna. A única possível quebra de privacidade seria no momento em que um usuário final decide disponibilizar, para análise da equipe de segurança, informações relacionadas a um ataque sofrido para que seja criada a proteção para aquele ataque. Porém, a contrapartida que se tem na proteção da comunidade sob a mesma equipe, além da proteção do próprio ecossistema da Internet compensam esta quebra de privacidade.	Consenso	Não Aplicável
Proposta	Pergunta: Como definir senhas seguras? E com qual Frequência trocá-las?	Consenso	Não Aplicável

	Pollyana Ringon: O principal ponto a se considerar para criar senhas fortes é evitar deixar brechas de engenharia social, não colocando informações associadas a você, seus familiares, ou seus interesses, para que alguém que queira te atacar não consiga adivinhar baseado em informações coletadas. Utilizar combinações de letras, números e caracteres especiais também ajuda. Também é importante evitar anotar as senhas em blocos de notas e afins. Já quanto ao período de troca de senhas, apesar do ideal ser manter trocas frequentes a cada 1 ou 2 meses, sabe-se que na maior parte dos casos isto é impraticável. O caminho então é tentar manter trocas a cada 6 meses, e trocar em períodos menores no caso de senhas de contas mais críticas. Claudio Miceli: Também é bom evitar criar senhas relacionadas entre si, já que caso uma das suas senhas seja descoberta, não seria difícil utilizar-se dela para chegar nas outras senhas similares.		
Posicionamento	Pergunta: A anatel ou as empresas pensam em algo para garantir um serviço mais prolongado em segurança. Pq tipo uma geladeira pode ter uma vida útil bem longa e no fim da sua vida o software pode estar inseguro? Thiago Barçante: A ANATEL exige que todos os dispositivos a serem comercializados passe pela sua homologação, a qual se repete frequentemente para assegurar que o dispositivo se mantém seguro. Caso alguma falha seja detectada, a ANATEL pode suspender a homologação e assim impedir a comercialização do dispositivo. Além disso, a ANATEL recomenda que o fabricante também especifique por quanto tempo o fabricante deseja manter suporte a atualizações de segurança destes dispositivos para que o consumidor consiga consultar e escolher de acordo com sua necessidade.	Consenso	Não Aplicável