RNP
REDE NACIONAL DE ENSINO E PESQUISA

ACORDO DE COOPERAÇÃO TÉCNICA PARA PESQUISA E DESENVOLVIMENTO

Pelo presente Instrumento particular e na melhor forma de direito, as Partes abaixo qualificadas resolvem celebrar o acordo de cooperação técnica, que entre si fazem mediante as cláusulas e condições que se outorgam e aceitam mutuamente, como adiante se segue.

CONTRATANTE: REDE NACIONAL DE ENSINO E PESQUISA – RNP, associação civil qualificada como Organização Social pelo Decreto nº 4.077, de 09 de janeiro de 2002, inscrita no CNPJ/MF sob o nº 03.508.097/0001-36, portadora da Inscrição Municipal nº 02.838.109, com sede na Rua Lauro Müller nº 116, 11º andar, salas 1.101 a 1.104, Botafogo, Rio de Janeiro/RJ, neste ato, representada por seu Diretor Geral, Nelson Simões da Silva, brasileiro, casado, engenheiro, portador da Carteira de Identidade nº 06.074.778-9, expedida pela IFP/RJ, inscrito no CPF/MF sob o nº 708.191.577-91, doravante denominada simplesmente **RNP**.

CONTRATADA: UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL – UFMS, Instituição de Ensino Superior sob a forma de Autarquia em Regime Especial, vinculada ao Ministério da Educação – ME, inscrita no CNPJ/MF sob o nº 15.461.510/0001-33, com sede na Av. Costa e Silva, CXPST 549, próximo Vila Ipiranga, Campo Grande/MS, CEP 79070-900, neste ato representada por seu Reitor, Marcelo Augusto Santos Turine, brasileiro, casado, bacharel em ciências da computação, portador da carteira de identidade nº 16.103.320-9, expedida pelo SSP/SP, inscrito no CPF/MF sob o nº 070.327.978-57, doravante denominada simplesmente **UFMS**.

Com a interveniência da **FUNDAÇÃO DE APOIO À PESQUISA, AO ENSINO E À CULTURA – FAPEC,** fundação de direito privado sem fins lucrativos, estabelecida na Rua 9 de Julho nº 1922, Campo Grande/MS, CEP 79081-050, portadora da Inscrição Municipal nº 28.211.972-8, inscrita no CNPJ/MF sob o nº 15.513.690/0001-50, neste ato representada por seu Secretário Executivo, Herbert Assunção de Freitas, brasileiro, divorciado, administrador, portador da carteira de identidade nº 737.601 expedida pela SSP/MS, inscrito no CPF/MF sob o nº 474.598.911-34, doravante denominada, simplesmente, **FAPEC.**

CLÁUSULA PRIMEIRA – DO OBJETO E DOS DOCUMENTOS APLICÁVEIS

1.1 – O presente Acordo tem por objeto a execução de parte do projeto de pesquisa e desenvolvimento intitulado "Researching Internet Routing Security in the Wild", no contexto da Chamada **RNP-NSF** para Projetos de Pesquisa e Desenvolvimento em Segurança Cibernética, sob gestão da **RNP**.

COORDENADORIA JURÍDICA RNP

1.1.1 – As atividades decorrentes deste Acordo, a que a **UFMS** se obriga perante à **RNP,** serão desenvolvidas pela **Faculdade de Computação** (FACOM) da **UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL.**

CLÁUSULA SEGUNDA – DO PLANO DE EXECUÇÃO DO PROJETO

2.1 – Os seguintes documentos constituem o **Plano de Execução do Projeto** e são partes integrantes deste documento, como se neles estivessem transcritos, cujo teor as partes declaram ter pleno conhecimento:

Nº	DESCRIÇÃO
ANEXO I	Proposta Técnica Detalhada
ANEXO II	Cronograma Físico-Financeiro
ANEXO III	Cronograma de Atividades
ANEXO IV	Orçamento Detalhado Definitivo

2.2 – Em caso de condições ambíguas ou contraditórias constantes dos Anexos acima citados, fica desde logo, estabelecido que sejam adotadas todas aquelas contidas neste Acordo.

2.3 – Os serviços serão considerados executados somente quando forem alcançados os resultados fixados nos Anexos acima mencionados.

2.4 – Os resultados parciais serão considerados concluídos após o atendimento das seguintes condições:

a) Mediante informação da **UFMS** de que os serviços relativos àquela etapa foram concluídos, devendo tal informação estar acompanhada de toda documentação associada.
b) Mediante a emissão do documento de aceite pela **RNP** dos serviços previstos para a etapa a que se referir.

2.5 – A **RNP** reserva-se o direito de, durante a execução do projeto, promover visitas técnicas ou solicitar informações adicionais, visando a aperfeiçoar o sistema de Avaliação e Acompanhamento.

CLÁUSULA TERCEIRA – DA VIGÊNCIA

3.1 – O prazo de vigência do presente Acordo é de 24 (vinte e quatro) meses, contados a partir da data de assinatura, podendo ser prorrogado por acordo das Partes mediante celebração de Termo Aditivo, caso haja necessidade devidamente justificada.

3.2 – Fica acordado que o término do prazo estabelecido no item 3.1 acima não exime as Partes de cumprirem com suas obrigações e responsabilidades assumidas durante a vigência deste Acordo.

COORDENADORIA JURÍDICA RNP

CLÁUSULA QUARTA – VALOR E CONDIÇÕES DE PAGAMENTO

4.1 – A **RNP** pagará a **FAPEC,** pela regular e completa execução dos serviços, objeto do presente Acordo, o valor total de R$ 278.306,32 (duzentos e setenta e oito mil, trezentos e seis reais e trinta e dois centavos), a serem pagos em parcelas trimestrais conforme cronograma de desembolso constante do Anexo II – Cronograma Físico-Financeiro, após validação dos resultados parciais, em conformidade com os termos da cláusula segunda. Adicionalmente, serão disponibilizados pela **RNP** e mantidos na **RNP** o montante de R$ 178.736,84 (cento e setenta e oito mil, setecentos e trinta e seis reais e oitenta e quatro centavos) para aquisição de equipamentos conforme previsão detalhada no Anexo IV.

4.2 – Quando solicitada, a **FAPEC** deverá enviar Nota Fiscal Eletrônica - NF-e para o e-mail nfe@rnp.br conforme cronograma de desembolso constante no Anexo II, devidamente firmada e cumpridas todas as exigências legais, cabendo à **RNP** a retenção e o recolhimento do IR e INSS ou quaisquer outros tributos que a lei assim o determine. Deverá ser apresentada a comprovação do recolhimento das contribuições sociais e dos documentos fiscais referentes aos serviços prestados no período.

4.2.1 - Nas localidades onde ainda não haja implantação de NF-e a **FAPEC** deverá encaminhar a Nota Fiscal para Av. André Tosello, nº209, Prédio da Embrapa/Unicamp, Caixa Postal 6001, 13083-886 Campinas, SP.

4.2.2. Caso a **FAPEC** seja optante pelo SIMPLES deverá encaminhar uma declaração.

4.3 - Estão inclusos no valor acima expresso todos tributos e encargos devidos, tais como, emolumentos, contribuições parafiscais, bem como outras de qualquer natureza que sejam devidas em decorrência direta ou indireta da execução do presente Acordo.

4.3.1 – Não serão efetuados quaisquer pagamentos enquanto perdurar pendências de liquidação de obrigações legais ou contratual.

4.4 – No caso de irregularidade na Nota Fiscal Eletrônica – NF-e esta será devolvida a **FAPEC** para as devidas correções, sendo tido como não apresentado, contando novo prazo, quando de sua reapresentação.

4.5 – Os pagamentos ocorrerão nos dias 15 ou 30, de cada mês subsequente ao da prestação dos serviços, sempre considerando a antecedência de 15 (quinze) dias para apresentação da NF-e.

4.6 – Fica desde já estabelecido que a **RNP** não se responsabilizará pelo pagamento de parcelas contratuais negociadas pela **FAPEC** junto à rede bancária, empresas de *factoring* ou outras instituições semelhantes, como descontos e cobrança de duplicata ou qualquer outra operação financeira, ficando a **FAPEC** com a responsabilidade sobre todas as despesas judiciais e cartorárias, caso sejam necessárias para a solução de

COORDENADORIA JURÍDICA RNP

qualquer conflito, mais multa não compensatória no valor de 20% (vinte por cento) sobre o montante do valor negociado.

4.7 – As despesas para fins de ressarcimento de custos incorridos pela executora, fundações ou outras instituições intervenientes, limitam-se à dez por-cento (10%) do custo total do projeto.

4.8 – Os repasses de recursos da **RNP** para a contratada ficarão condicionados ao efetivo repasse de recursos por parte da Secretaria de Políticas de Informática (SEPIN/MCTI) à **RNP**, bem como à regularidade do credenciamento da unidade acadêmica executora, indicada no item 1.1.1 deste Acordo, no Comitê da Área de TI (CATI). Comprovando assim, ser uma unidade habilitada à execução de atividades de pesquisa e desenvolvimento, para os fins previstos nos incisos I e II do § 1o do art. 11 da Lei no 8.248, de 23 de outubro de 1991.

CLÁUSULA QUINTA – DAS DESPESAS NA EXECUÇÃO DOS SERVIÇOS

5.1 – As despesas decorrentes da execução deste Acordo, tais como recursos materiais essenciais, suporte administrativo e infraestrutura de informática que não estejam contemplados nos Anexos deste Acordo, serão de responsabilidade da contratada/instituição de execução do projeto, a título de contrapartida.

CLÁUSULA SEXTA – DO SIGILO E CONFIDENCIALIDADE

6.1 – As Partes se comprometem a manter sigilo e confidencialidade de todo o teor das informações a que tiver acesso por força deste Acordo, sob pena de responder pelos danos e prejuízos decorrentes da divulgação indevida.

6.2 – O sigilo e a confidencialidade previstos nesta Cláusula aplicam-se, inclusive e especialmente, ao *know how* referente ao objeto deste Acordo utilizado na prestação dos serviços, que por força deste Acordo venha a ser conhecido pela outra Parte e eventualmente compartilhado entre si durante a sua execução.

> 6.2.1 – Para fins deste Instrumento, entende-se por *know how* o conhecimento não protegido por patentes ou qualquer outro direito de propriedade de acesso extremamente restrito passível de ser retransmitido e que, quando aplicado ao processo produtivo ou execução de serviços a que se destina, implique vantagem para o seu titular.

6.3 – As Partes, em virtude do acesso recíproco que terá às informações privilegiadas ou confidenciais da **RNP**, obrigam-se a:

a) Não permitir o acesso às informações confidenciais da outra Parte a terceiros não credenciados, incluindo representantes, agentes, consultores e estes apenas na extensão necessária para permitir a concretização do objeto deste Acordo;

COORDENADORIA JURÍDICA RNP

b) Não utilizar qualquer das informações referente aos produtos gerados para entrega do objeto deste Acordo, exceto para os fins previstos no objeto deste Acordo e/ou de outro acordo celebrado entre as Partes;

c) Manter a maior confidencialidade possível em relação às informações recebidas, inclusive zelando, com rigor, para que não haja circulação de cópias, e-mails, fax ou outras formas de comunicação privada ou pública das informações, além da estritamente necessária para o cumprimento do objeto deste Acordo.

6.4. As Partes declaram que não constituem infração ao disposto no item 6.3 acima, nas hipóteses em que:

a) A informação torna-se disponível ao público em geral por meio que não resulte de sua divulgação pelas Partes ou de seus representantes;

b) A revelação seja exigida por autoridade governamental ou ordem de Tribunal competente, sob pena de ser caracterizada a desobediência ou outra penalidade. Nessas hipóteses o material a ser revelado deverá ser objeto de toda proteção, governamentais ou judiciais aplicáveis, devendo a Parte que estiver obrigada a revelar tais informações comunicar antecipadamente, por escrito, a outra Parte, dando ciência de qual a informação que será revelada;

c) A revelação for previamente autorizada pela outra Parte e por escrito.

6.5 – Entende-se por informações confidenciais ou privilegiadas todas as informações e documentos de quaisquer espécies, que sejam entregues a uma das Partes pela outra, por seus consultores, auditores, advogados, contadores, representantes e empregados e que estejam relacionados aos negócios das Partes ou aos negócios de seus parceiros, fornecedores e associados.

6.6 – As Partes deverão instruir todos aqueles a quem fornecer acesso às informações confidenciais da **RNP** sobre a obrigação de sigilo e de não divulgação ora assumidas.

6.7 – As Partes reconhecem que todas as informações confidenciais fornecidas pela **RNP** para desenvolvimento das atividades estabelecidas no objeto deste Acordo, constituem propriedade exclusiva da **RNP** e que sua revelação não implica, de forma alguma, licença, autorização, concessão, cessão, transferência, expressa, tácita ou implícita, de qualquer direito autoral, de propriedade intelectual, idéia, conceito, marca, patente ou de outro direito de titularidade da **RNP**.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DAS PARTES

7.1 – Cabe a **RNP**, além das demais obrigações já estabelecidas neste Acordo, as seguintes:

a) Fornecer as informações, documentos, e dados, colocando à disposição da **UFMS** todos os meios necessários à realização dos serviços ora estipulados;

COORDENADORIA JURÍDICA RNP

b) Efetuar os pagamentos dentro do estabelecido no item 4.1 da Cláusula Quarta deste Acordo;

c) Comunicar a **UFMS** e à **FAPEC**, sobre quaisquer irregularidades encontradas na execução do presente Acordo.

7.2 – Cabe a **UFMS** e à **FAPEC**, no que couber, além das demais obrigações já estabelecidas neste Acordo, as seguintes:

a) Receber visitas técnicas e prestar todos os esclarecimentos que forem solicitados pela **RNP**;

b) Utilizar exclusivamente para as atividades ora estipuladas, toda e qualquer informação e/ou documentos obtidos da **RNP** para fins deste Acordo, sob pena de responder pelos danos e prejuízos decorrentes da divulgação indevida;

c) Levar imediatamente ao conhecimento da **RNP** qualquer fato extraordinário ou anormal que ocorra na execução de suas atividades que possa prejudicar o bom andamento dos serviços;

d) Refazer a tarefa quando o resultado apresentado não atingir as condições de aceitação estabelecidas, caso em que a **RNP** fundamentará os motivos ensejadores, e efetuará as correções necessárias às suas próprias expensas, sem prejuízo dos prazos estabelecidos e sem ônus adicional para a **RNP;**

e) Manter sigilo e confidencialidade de todo teor das informações fornecidas pela **RNP** a que tiver acesso por força deste Acordo, sob pena de responder pelos danos e prejuízos decorrentes da divulgação indevida;

f) Observar, nas aquisições de serviços, os princípios da impessoalidade, moralidade, publicidade, eficiência e economicidade, adotando procedimentos que permitam identificar os preços médios de mercado e a obtenção de, no mínimo, orçamentos de 3 (três) fornecedores, salvo razões de ordem técnica ou de mercado, devidamente justificadas;

g) Manter cópias de todos os documentos de comprovação de despesas, suas autorizações e execuções, integralmente digitalizadas em repositório de banco de dados digital, com acesso amplo e imediato, devendo os documentos originais serem conservados em arquivo pelo prazo de 5 (cinco) anos a contar do fim da prestação de contas.

CLÁUSULA OITAVA – AQUISIÇÃO E USO DOS BENS PATRIMONIAIS

8.1 – A **RNP** disponibilizará à **UFMS** para seu uso exclusivo, a título de empréstimo e mediante assinatura de Termo de Responsabilidade, os bens adquiridos com recursos recebidos para implemento dos serviços ora ajustados, devendo a **UFMS**:

COORDENADORIA JURÍDICA RNP

a) Manter controle sobre os bens disponibilizados pela **RNP** às suas subcontratadas indicando essa situação quando solicitado pela **RNP**;

b) Comunicar à **RNP**, imediatamente, qualquer dano que os referidos bens vierem a sofrer;

c) Assegurar a adequada operação dos bens adquiridos, promovendo a execução dos reparos e substituições necessárias, e arcar com todas as despesas referentes ao transporte, guarda, conservação, manutenção e recuperação, sem que lhe caiba direito a retenção ou a qualquer indenização;

d) Informar à **RNP** a devolução de quaisquer bens, em razão da conclusão do serviço ou da sua não utilização;

e) Em caso de furto ou de roubo do bem, promover o registro da ocorrência perante a autoridade policial competente, enviando cópia da ocorrência à **RNP** e diligenciando para que se proceda à investigação pertinente.

f) Responder anualmente o Inventário de Bens **RNP**, informando o status atualizado dos materiais, mediante solicitação formal com antecedência de 30 (trinta) dias.

CLÁUSULA NONA – COORDENAÇÃO E OPERACIONALIZAÇÃO DOS SERVIÇOS

9.1 – As Partes indicarão seus respectivos Coordenadores através de correspondência a ser firmada, os quais terão amplos poderes para adotarem as providências necessárias para o bom andamento dos serviços e atividades deste Acordo.

9.2 – Todas as requisições, envio de documentos e comunicações referentes ao presente Acordo deverão ser feitas através dos Coordenadores indicados.

CLÁUSULA DÉCIMA – DA DISSOLUÇÃO CONTRATUAL

10.1 – Este Acordo será rescindido de pleno direito caso ocorra a insolvência civil ou a paralisação das atividades de quaisquer das Partes e, também, pelo descumprimento de qualquer das cláusulas e condições ora estipuladas, com ressalva nos casos fortuitos ou de força maior e das disposições do artº 399 do Código Civil.

10.2 – É facultado a qualquer uma das Partes resilir o presente Acordo a qualquer tempo, independentemente de interpelação ou notificação judicial ou extrajudicial, desde que seja feita a comunicação, por escrito, com antecedência mínima de 30 (trinta) dias.

CLÁUSULA DÉCIMA PRIMEIRA – DA PROPRIEDADE DOS RESULTADOS

COORDENADORIA JURÍDICA RNP

11.1 – Todos os resultados intermediários e finais, privilegiáveis ou não, envolvendo invenções, processos, métodos, programas de computador ou inovações técnicas, passíveis de proteção ou não, obtidos em virtude da execução deste Acordo, terão seus direitos divididos entre as partes na proporção e forma estabelecidas em instrumento específico.

11.2 – Para resultados intermediários e finais obtidos em virtude da execução deste Acordo, a **RNP** recomenda que sejam divulgados somente após o protocolo de pedido de proteção, para que o requisito de novidade seja mantido.

11.3 – Todos os resultados intermediários e finais, privilegiáveis ou não, envolvendo invenções, processos, métodos, programas de computador ou inovações técnicas, passíveis de proteção ou não, obtidos em virtude da execução deste Acordo, com potencial de aplicação e de interesse por terceiros, terão sua transferência estabelecida em instrumento específico entre as partes.

11.4 – A **UFMS** assume total responsabilidade pela originalidade e propriedade do texto e das ilustrações utilizadas no objeto do presente Acordo, ficando desde já obrigado a fornecer à **RNP** a devida e legal autorização de permissão de uso.

CLÁUSULA DÉCIMA SEGUNDA– MÃO-DE-OBRA FORNECIDA

12.1 – A mão-de-obra fornecida pelo **UFMS** para o desenvolvimento das atividades ora avençadas será de sua única e exclusiva responsabilidade, não ensejando qualquer vínculo contratual com a **RNP.**

CLÁUSULA DÉCIMA TERCEIRA – DA PROPRIEDADE INTELECTUAL E INDUSTRIAL

13.1 – As Partes retêm, individualmente, seus respectivos direitos de propriedade intelectual e industrial, já existentes e utilizados nas obras criadas, desenvolvidas ou modificadas durante a vigência deste Acordo;

13.2 – Nenhum direito de propriedade intelectual e industrial, atualmente existente ou que venham a ser adquiridos ou licenciados por uma Parte, será outorgado à outra Parte.

13.3 – As marcas e patentes pertencentes a uma Parte e que forem necessárias à outra Parte para o cumprimento das atividades previstas neste Acordo (uso de quaisquer facilidades ou equipamentos, incluindo programas/*software)* somente poderão ser utilizados mediante expressa autorização da Parte detentora dos direitos.

13.4 – Cada Parte será responsável, sem nenhum custo adicional à outra Parte, pela obtenção de licenças relativas à propriedade intelectual e/ou industrial usada para o cumprimento de suas respectivas obrigações na vigência deste Acordo.

13.5 – Salvo acordo em contrário e específico, celebrado entre a **UFMS**, a **FAPEC** e a

COORDENADORIA JURÍDICA RNP

RNP, nenhuma das Partes poderá publicar ou usar logotipo, marcas registradas (incluindo marca de serviço) e patentes, nome, redação, fotos/quadros, símbolos ou palavras da outra Parte, através das quais possa o nome da outra Parte ser associado em qualquer produto, serviço, promoção ou qualquer outra matéria de publicidade.

CLÁUSULA DÉCIMA QUARTA – DAS DISPOSIÇÕES GERAIS

14.1 – A inaplicabilidade ou nulidade de quaisquer dos termos e condições ora ajustadas, não resultará na nulidade das demais cláusulas que continuarão em plena vigência e eficácia até o término ou rescisão deste Acordo.

14.2 – Quaisquer alterações e complementações às cláusulas ora ajustadas, somente terão validade quando feitas por escrito, na forma de Termos Aditivos, assinados pelos representantes legais das Partes.

14.3 – Em caso de divergência entre as disposições, prevalecerão as estabelecidas na seguinte ordem: O Aditivo mais recente sobre o mais antigo; o presente Instrumento e seus anexos.

14.4 – Não valerá como precedente, novação ou renúncia, aos direitos assegurados a cada uma das Partes, pela Lei e pelo presente Instrumento, a tolerância de uma das Partes quanto a eventuais descumprimentos ou infrações às condições aqui estabelecidas, as quais poderão ser exigidas a qualquer tempo.

14.5 – As Partes declaram concordar expressamente com os termos ora ajustados, obrigando-se mutuamente pelos direitos e obrigações decorrentes deste Acordo, bem como, eventualmente, seus assessores, a qualquer título.

14.6 – Cabe a **UFMS** e à **FAPEC** responder civilmente por quaisquer erros ou danos comprovados como de sua responsabilidade, que representarem prejuízos para a **RNP** e sejam decorrentes de procedimento realizado ou comportamento de seus empregados, representantes ou prestadores de serviços, no ambiente de trabalho, junto às diversas interfaces profissionais e demais instituições, além da própria **RNP**.

14.6.1 – Em tais hipóteses, deverá a **UFMS** e à **FAPEC** ressarcir 20% (vinte por cento) do valor pago do Acordo, além de responder pela reparação pública, por escrito, quanto aos motivos da falha e isenção da **RNP**.

CLÁUSULA DÉCIMA QUINTA – DA RESPONSABILIDADE SOCIAL

15.1 – Das Obrigações para não adoção de práticas de trabalho ilegal:

15.1.1 – A **UFMS** se compromete a não adotar práticas de trabalho análogo ao escravo e trabalho ilegal de crianças e adolescentes no cumprimento do presente Acordo.

15.1.2 – A **UFMS** se compromete a não empregar trabalhadores menores de 16 (dezesseis) anos de idade, salvo na condição de aprendiz a partir de 14 (quatorze)

COORDENADORIA JURÍDICA RNP

anos de idade, nos termos da Lei nº 10.097, de 19.12.2000, e da Consolidação das Leis do Trabalho.

15.1.3 – A **UFMS** se compromete a não empregar adolescentes até 18 (dezoito) anos de idade, em locais prejudiciais à sua formação, ao seu desenvolvimento físico, psíquico, moral e social, bem como, em locais e serviços perigosos ou insalubres, em horários que não permitam a frequência à escola e, ainda, em horário noturno, considerado este o período compreendido entre as 22:00 h às 05:00 h.

15.2 – Das obrigações para proteção e preservação do meio ambiente:

15.2.1 – A **UFMS** se compromete a proteger e preservar o meio ambiente, bem como a prevenir contra práticas danosas ao meio ambiente, executando seus serviços em observância dos atos legais, normativos e administrativos relativos à área de meio ambiente e correlatas, emanadas das esferas Federal, Estaduais e Municipais, incluindo, mas não limitando ao cumprimento da Lei Federal nº 6.938/81 (Política Nacional do Meio Ambiente) e da Lei nº 9.605/98 (Lei dos Crimes Ambientais), implementando ainda esforços nesse sentido junto aos seus respectivos fornecedores de produtos e serviços, a fim de que esses também se comprometam a conjugar esforços para proteger e preservar o meio ambiente, bem como a prevenir contra práticas danosas ao meio ambiente, em suas respectivas relações comerciais.

15.2.2 – Respeitar e cumprir, rigorosamente, o disposto na Legislação Ambiental vigente, responsabilizando-se perante a **RNP** os Órgãos Ambientais e terceiros por todos e quaisquer danos e prejuízos que, por sua culpa ou omissão, inclusive de seus prepostos, venha causar ao meio ambiente.

15.2.3 – Observar e fazer cumprir as disposições da Portaria n.º 85, de 17 de outubro de 1996, do IBAMA, diligenciando para que a emissão da fumaça preta dos veículos no transporte utilizado fique dentro do limite permitido.

15.3 – É facultado à Contratante verificar o cumprimento das disposições contidas nesta Cláusula, cujo descumprimento, por parte da Contratada, ensejará justo motivo para a rescisão do presente Acordo.

15.4 – A presente cláusula também se aplica ao zelo que a **RNP** terá com seus fornecedores, no que diz respeito ao processo produtivo, serviços, produtos utilizados e descarte.

CLÁUSULA DÉCIMA SEXTA – DO FORO

16.1 – Fica eleito o foro da Justiça Federal, Seção Judiciária cidade do Rio de Janeiro (RJ), com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir as dúvidas ou controvérsias do presente Acordo.

COORDENADORIA JURÍDICA RNP

E, por estarem de pleno acordo, assinam o presente Acordo em 04 (quatro) vias de igual teor e forma, na presença das testemunhas, uma de cada instituição, ao final nomeadas.

Rio de Janeiro, 02 de outubro 2017

REDE NACIONAL DE ENSINO E PESQUISA – RNP
Nelson Simões da Silva
Diretor Geral

Testemunha RNP:

Nome: Wanderson Paim de Jesus
CPF: 024.807.851-81

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL – UFMS
Marcelo Augusto Santos Turine
Reitor

FUNDAÇÃO DE APOIO À PESQUISA, AO ENSINO E À CULTURA – FAPEC
Herbert Assunção de Freitas
Secretario Executivo

Testemunha UFMS:

Nome Ronaldo Alves Ferreira
CPF: 558.742.741-20

Testemunha FAPEC:

Nome Glenda M Lemanji
CPF: 009026541-60

COORDENADORIA JURÍDICA RNP

FL Nº 23
6
PROPP

EAGER:USBRCCR: Researching Internet Routing Security in the Wild

Principal Investigators: Ethan Katz-Bassett (Columbia University, USA)
Ítalo Cunha (Universidade Federal de Minas Gerais, Brazil)
Researchers: Cristine Hoepers, Klaus Steding-Jessen (NIC.br)
Dorgival Guedes, Wagner Meira Jr. (Universidade Federal de Minas Gerais)
Ronaldo Ferreira (Universidade Federal de Mato Grosso do Sul)

Summary

The Internet provides a control plane to establish routes to destinations and a data plane to send traffic, and the protocols for both lack authentication. The lack of authentication allows networks to claim ownership of routes to other networks' addresses in order to siphon traffic (Border Gateway Protocol prefix hijacking), and allows hosts to claim that their traffic came from a different source (source spoofing). These vulnerabilities form the basis for denial-of-service attacks, traffic interception and snooping, Bitcoin theft, and compromises of Tor's anonymity.

Because of these vulnerabilities and the centrality of the Internet in today's world, routing research is a critical aspect of cybersecurity research. However, researchers cannot perform Internet routing experiments that are both controlled and realistic: existing measurement techniques measure routes as-is, without control, and limitations in our ability to measure the Internet mean that simulations lack realism. Uncontrolled measurements of the Internet as-is cannot differentiate between competing explanations for observed routes, and so current techniques cannot achieve accuracy, precision, and coverage in measuring which networks allow spoofed traffic or hijacked routes. A researcher could achieve realism and control if a network operator ceded control of the network's routing and traffic. We are left with a Catch-22: without real-world evaluation, networks are unlikely to deploy approaches proposed by researchers; without deployment, researchers cannot conduct real-world evaluation.

Intellectual merit. This project aims to (1) enable classes of security-focused routing research that are beyond the reach of academic researchers today, via extending the PEERING testbed, and to subsequently (2) develop techniques that use the testbed to identify which networks allow data and control traffic that uses unauthorized IP addresses.

PEERING is an interdomain routing research platform we developed that gives researchers control of a network in the Internet, with routers spread across four continents directly connected to hundreds of real networks. We propose extensions that will help security researchers design and evaluate solutions in realistic scenarios, emulating attacks and running prototypes on the actual Internet.

We then propose to use the extensions to study routing security issues. On the control plane, we will characterize deployment of RPKI Route Origin Validation, which has the potential to limit prefix hijacks. On the data plane, we will develop techniques to locate the networks that allow packets with spoofed sources. Our techniques will use PEERING's ability to manipulate routing to observe how route changes impact the volume of spoofed traffic received from each peer and which vantage points do/do not use invalid routes. By changing routing, we can narrow the set of feasible explanations to those consistent with all observations, yielding more precise inferences. We will have to address challenges including limited visibility of Internet routes, lack of ground truth about routing policies, and lack of control of routing decisions of other networks.

Broader impact. Internet routing is a critical component of cybersecurity. Our studies of the sources of spoofed traffic and deployment of hijack prevention will be useful to researchers and network operators. The studies will help locate susceptible networks, more precisely map bot populations, and serve as a step towards mitigation; will evaluate the impact over time of efforts by routing registries, vendors, and operator organizations to encourage security adoption; may inform policymakers, improve best practices, and encourage adoption; and can reveal topics worthy of further study and support the development of new countermeasures to attacks. We will work with operators to transition our techniques and results into practice. Our extensions to PEERING will empower novel research by other researchers, particularly the security community. We will continue to give talks about our results and the PEERING testbed in conferences, universities, operator meetings, and workshops; use the platform in courses; and improve documentation.

Keywords. Internet, routing, security, prefix hijacks, DDoS, RPKI, IP source spoofing, community testbed.

Fl. Nº 24
PROPP

Broader impact. The rise of applications that use sensitive data and our increased dependence on the Internet mean that it is critical to understand and improve Internet routing as a component of cybersecurity.

Our studies of the sources of spoofed traffic and deployment of hijack prevention can serve a number of purposes. The studies will help locate susceptible networks, more precisely map bot populations, and serve as a step towards mitigation; will evaluate the impact over time of efforts by routing registries, vendors, and operator organizations to encourage security adoption; may inform policymakers, improve best practices, and encourage adoption; and can reveal topics worthy of further study and support the development of new countermeasures to attacks.

We expect providers to benefit from our approaches, and we will work with them to transition the techniques and results into practice. We will make our measurements and measurement platforms available to researchers, providing a novel view of important aspects of today's Internet, spurring research. Results from this project can be used by researchers, network operators, and standards bodies, informing policies against Internet resource abuse (e.g., prefix hijacks), standardization efforts in the IETF, or the ongoing debate about IoT security. We will continue our dissemination of routing research by presenting at network operator conferences (NANOG, RIPE) and standards bodies (IETF), and we will start a similar effort in Brazil.

Our proposed work will have additional broader impact beyond the results of our concrete research studies, as our extensions to the PEERING testbed will open the testbed to the security research community, empowering novel research by others. The proposed extensions will *make PEERING a unique tool for the community to tackle current Internet security challenges and an asset against security challenges to come.* We will continue to give frequent short advertisement talks about the testbed at research institutions and conferences to drive testbed use, as well as co-organize BGP hackathons like the 2016 one which introduced 90 participants to PEERING and other BGP tools. We will develop course projects that use the testbed to investigate spoofing and hijacking, and we will make the materials publically available. Finally, this project will foster cooperation between multiple groups in the US and Brazil. The Brazilian government is trying to expand the research contribution of the state that includes UFMS (one of the institutes of our proposal) in order to encourage research nationwide and reduce inordinate concentration of education and research.

EAGER rationale. *Reward:* Researchers traditionally have no control of the Internet's routing ecosystem, limiting research to passive routing observations. PEERING allows active routing research on the Internet, revolutionizing the capabilities available to researchers, with two aspects in particular amplifying the potential impact of the proposed work. First, as a community testbed, it opens a pathway to groundbreaking work by others, in addition to our work. Second, because PEERING is an actual network connecting to other real networks across the Internet, the results are realistic and can be directly applicable to the Internet.

Risk: The two aspects that increase the possible reward also add risks beyond the uncertainty intrinsic in all exploratory research. First, a community testbed is only useful if the functionality is useful to and used by others. We need to develop scalable mechanisms to support rich functionality such as on-path packet processing, a challenge since deploying fast network processing on commodity servers is an active area of research [40, 59]. We will only be able to enable useful but potentially risky functionality such as sending (carefully controlled) spoofed traffic or hijack announcements if we develop ways of isolating the Internet from errant experiments. We also need to attract researchers to use it.

Second, the precision of our proposed techniques to locate networks that allow spoofed traffic or filter invalid routes depends on the degree to which we can manipulate routing to rule out alternate explanations for measurements. The techniques could fail to yield suitably precise inferences, depending on the peering connectivity of the testbed and how it relates to the policies and topologies of the rest of the Internet. Until we run experiments in the wild, we cannot know whether we can attain sufficient precision, due to the challenges of modelling the Internet's policies and topologies. The coverage and representativeness of other PEERING-based experiments are also tied to the peering connectivity of the testbed. We describe our efforts to mitigate these risks by attracting users in **Broader impact** above and by expanding coverage in §3.3.[1] With users and rich connectivity, this project will contribute to network research and operations and to improving routing security, benefitting service providers and users.

Team. This project will build on the PIs' expertise on Internet routing, measurement, and experimentation platforms. PI Katz-Bassett has extensive experience on Internet measurement and routing [10, 11, 84, 87, 39,

[1] Infrastructure expansion is supported by a separate infrastructure grant CNS-1406042 and by the Brazilian budget.

FL Nº 25
PROPP

2.1 Tracking adoption of Route Origin Validation (ROV)

A proposal to improve routing security—Route Origin Authorization (ROA)—has been standardized. A ROA specifies which network is allowed to announce a set of Internet destinations. While some networks now specify ROAs, little is known about whether other networks check routes they receive against these ROAs, a process known as Route Origin Validation (ROV). Which networks blindly accept invalid routes? Which reject them outright (`filter-invalid`)? Which de-preference them if alternatives exist (`prefer-valid`)?

A recent approach attempts to characterize ROV adoption in unvalidated, uncontrolled experiments by comparing routes to valid origins versus routes to existing invalid routes [33]. Our measurements demonstrate three major problems with the approach that are fundamental to uncontrolled experiments. First, the paper makes its characterizations based on routes from an unspecified subset of available vantage points, but our measurements show the approach's characterization of some networks changes depending on which subset is used, with some cases likely false positives and some false negatives. Second, the paper relies on invalid routes that happen to be announced, and so its coverage is limited by their rare nature. Third, we conducted supplemental measurements that suggest that most networks flagged by the approach (and by [33]) as using ROV are actually avoiding invalid routes for unrelated (non-security) traffic engineering purposes, without checking ROV status. In fact, with only uncontrolled measurements of existing routes–the status quo for Internet research–it is impossible to differentiate between multiple feasible explanations.

To fill this knowledge gap, we will develop a methodology to accurately infer filtering policies using controlled experiments that use PEERING to jointly manipulate BGP announcements and the ROAs that apply to them. We will conduct a longitudinal study of adoption of ROV across the Internet.

Challenges and requirements:

- *Experiments must be long-lived.* Adoption is likely to be slow, and it may be bursty, driven by various initiatives and technologies. Measurements must be rerun periodically.
- *Experiments must be active and controlled.* Passive observation of existing announcements may not test a policy, and available route collectors may not provide the right vantage to locate filtering. We must coordinate BGP announcements with ROA manipulations to precisely exercise behavior.
- *Experiments require competing announcements.* To identify `prefer-valid` policies, we need multiple simultaneous announcements for the same addresses. Since a single BGP session generally allows only a single announcement, the experiment must include sessions with multiple peers.
- *Experiments require rich BGP connectivity.* From a single vantage point, it is impossible to tell which network along a path is filtering an announcement.

Basic approach: The goal of each experiment is to understand the ROA/ROV policies of one target network. We first describe the experiment making two assumptions about the target network **N**:

- [`connected-assumption`] We assume **N** has a direct peering established with PEERING.
- [`visibility-assumption`] We assume we can check the BGP route **N** uses to reach an Internet destination, either via a Looking Glass server or a route collector (e.g., RIPE RIS [70]).

PEERING connects to other networks via AS47065, but it can use ASNs **D** and **T** as "customers" of AS47065. Our experiments will use ASN **D** to originate routes that AS47065 announces directly to **N** and use ASN **T** to originate routes that AS47065 announces via transit. We will test these configurations:

- [**D** and **T** both announce prefix $\mathbf{P_0}$, no ROA]
- [Only **D** announces $\mathbf{P_1}$, ROA specifies **T** is valid]
- [**D** and **T** both announce $\mathbf{P_2}$, ROA specifies **T**]

$\mathbf{P_0}$ establishes a baseline as to whether **N** prefers to route via **D** in the absence of ROA. If not, we can make **T**'s route less attractive by prepending it or announcing it via different transit. By checking which origin **N** selects for combinations of other prefixes, we can establish its ROA policy:

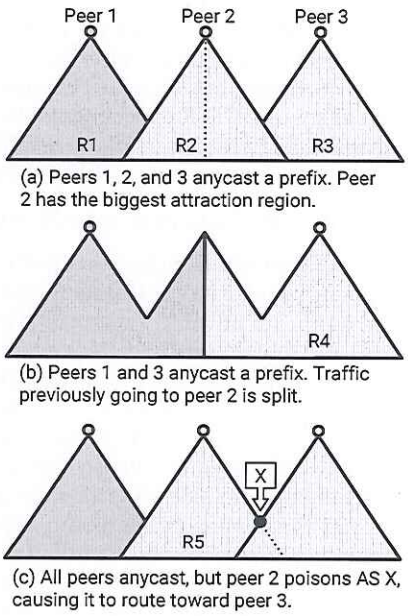
- [No route for $\mathbf{P_1}$, **T** for $\mathbf{P_2}$] **N** uses `filter-invalid` policy.
- [**D** for $\mathbf{P_1}$, via **T** for $\mathbf{P_2}$] **N** uses `prefer-valid` policy.
- [**D** for $\mathbf{P_1}$, **D** for $\mathbf{P_2}$] **N** does not consider ROA compliance in route selection.

There are subtleties in checking `prefer-valid` policies, as **N** is "allowed" to use ROA status as one part of checking how preferred a path is, but, for example, it may prefer invalid peer routes over valid provider routes but not over valid peer routes. We will explore how best to capture these policies, building on our work on using PEERING to uncover (non-security-related) routing policies [4].

FL Nº 26
PROPP

change in attack volume at each ingress. In Figure 1(b), the prefix is announced only to peers 1 and 3, resulting in different routing decisions and traffic attraction regions. We can directly measure the volume from R_4, and we can also use set algebra to infer the volume from smaller subregions. For example, the left half of R_2 is $R_2 + R_3 - R_4$. In Figure 1(c), the announcement through peer 2 poisons AS X, which triggers BGP loop prevention and makes AS X choose a route toward peer 3 instead. The traffic coming from ASes below AS X is $R_2 - R_5$. We will build on our work that manipulates announcements to infer policies [43, 4].

Improving speed. For location information to help mitigate an attack, the search has to be fast. It is infeasible to try announcements exhaustively, given the exponential number of possible announcements as well as delays imposed by BGP convergence and route-flap dampening [50, 47, 28]. We will develop techniques to choose and sequence announcements to quickly converge on attack origins. The problem is challenging because it is hard to predict the outcome of an announcement.



(a) Peers 1, 2, and 3 anycast a prefix. Peer 2 has the biggest attraction region.

(b) Peers 1 and 3 anycast a prefix. Traffic previously going to peer 2 is split.

(c) All peers anycast, but peer 2 poisons AS X, causing it to route toward peer 3.

Figure 1: Each subfigure represents one set of announcements. Colored regions indicate Internet hosts routing via Peer 1/2/3. Varying announcements causes shifts in the set of hosts downstream from a Peer, influencing how much attack traffic we measure at each Peer.

2.3 Evaluation plan for both techniques

Precision: When we observe ROV filtering on a path to a network not connected to PEERING, or when narrowing down the origin of spoofed traffic, we may only be able to narrow down the source to a set of networks rather than a single one. We will assess the distribution of the sets' sizes and investigate their relationships to routing policies and route diversity.

Accuracy: We will contact network operators to verify our observations that they deployed ROV/BCP38. By contacting them from PEERING's network operations center, we expect a higher response rate than typically achieved by academic researchers. We will characterize improvements versus an existing approach [33]. We will also evaluate on a range of emulated topologies.

Coverage: Our techniques try to isolate networks' decisions by tailoring BGP announcements from PEERING, then measure the routes from those networks to infer policy. The coverage depends on (a) which networks we can target with announcements, which depends on PEERING's interconnectivity and choices made by networks between PEERING and the target; and (b) which networks we can measure routes from, which depends on available vantage points and measurement approaches. We will evaluate the fraction of networks that we can target with announcements and for which we can measure routes. We will also compare to existing approaches [7, 33]. §3.3 describes our efforts to improve coverage.

Speed: Our techniques manipulate BGP announcements to narrow the number of possible explanations. We will evaluate the relationship between the number of announcements and the precision achieved.

3 Proposed Work: Extending PEERING for Security Research

PEERING currently focuses on routing research, with the goal of providing researchers flexible control and visibility over routing. In 2016, more than 70% of the proposals we received from external researchers were security research. Most proposals focused on routing or forwarding attacks on applications, including Tor, domain certification, and Bitcoin, demonstrating widespread use cases of the testbed. Security research requires functionality PEERING does not readily provide today. *We will integrate new security-specific functionality, as well as functionality that will benefit a range of experiments, including security-related ones.*

3.1 Add security-specific functionality

Originate safe spoofed traffic. The ability to inject spoofed traffic would help researchers study its prevalence, reach, impact, and mitigation. We will investigate how to safely allow spoofed traffic to enable new

FL. Nº 27
PROPP

Monitor route visibility. We will develop a monitoring system that predicts which measurement points should receive particular PEERING route announcements, then compares the predictions to actual visibility to help locate (incorrect) route filters. For example, recently PEERING prefixes were being filtered by (indirect) providers three AS-hops away, which is very hard to detect without automated testing. Such functionality could also be useful to network operators. We will also use the system to predict the increase in visibility and coverage attainable by adding particular peers, in order to prioritize peerings to pursue.

4 Related Work

Route origin validation and secure interdomain routing. The research and operator communities have proposed several approaches to secure routing in the Internet, from tools to detect BGP misconfigurations (and avoid accidental hijacks) [53, 27] to extending BGP to provide route authentication and verification [49, 9, 13]. Unfortunately, BGP authentication solutions like S-BGP, soBGP, BGPsec, and ROV have not gained significant traction [33, 36, 42], even though they have been shown useful in simulation [13, 37]. ROV [67] is the one approach currently seeing some deployment, While it does not prevent all attacks [33, 42, 13], it presents an interesting trade-off between deployability and security [36]. Our RPKI characterization will complement existing research and drive adoption by tracking the current state of ROV deployment and the security it provides in practice.

Spoofed DDoS mitigation. Under BCP38's Reverse Path Filtering (RPF), a network only accepts packets from downstream customers if the packets' source addresses belong to prefixes actively advertised by those customers [64]. RPF is hard to configure at networks with large and dynamic sets of (indirect) customers. RPF requires wide adoption to be effective, as any networks that do not adopt can be used to target amplification servers for reflection attacks. Current commercial solutions do not prevent the attack, instead mitigating its impact by scrubbing traffic [2, 82, 80, 51] or dropping it [65]. Our techniques complement other research aiming at identifying the sources of attacks, e.g., through correlation of packet frequencies [83].

5 Results from Prior NSF Support

Ethan Katz-Bassett is the PI of *CNS-1351100: CAREER: Routing for the Emerging Topologies of Modern Internet Services ($623K, 2014-2019).* **Intellectual Merit.** The key results and goals are to understand and improve routing of large content providers (e.g., Google), by: developing techniques to locate servers and uncover client-to-server mappings [10, 25]; developing new techniques to measure their Internet routes [12, 4, 19]; building a new testbed to allow researchers to exchange routes/traffic with real networks around the world to enable new experiments in this setting [73]; measuring performance of providers [11, 84, 87, 39, 41, 88, 3, 30]; and proposing techniques to improve them [10, 11, 30]. **Broader Impact.** This project has significantly impacted the routing and performance of large content providers: PI Katz-Bassett advised his student Brandon Schlinker as he built the system that controls Facebook's Internet routing (paper under preparation); his student Matt Calder as he built the system that monitors and controls Microsoft's client-to-server mapping (paper under preparation); and his student Tobias Flach as he collaborated to build a pipeline to identify performance problems as Google serves clients [30]. This last project resulted in improvements to TCP, deployed at Google and upstreamed into linux [29, 30]. Measurement data from this project [10] has been accessed by over 200 individuals. Per contacts at Microsoft, results from the project have been presented to the highest levels of Microsoft management and have driven a lot of Microsoft's thinking in content delivery, as well as led to a collaboration between PI Katz-Bassett and Microsoft to assess the performance of their content delivery and propose and assess improvements [11]. Aspects of the work have been presented at industry conferences ONS 2014, NANOG 61, NANOG 66, NANOG 69, NANOG OTR 3, Global Peering Forum 11, and RAIM 2016, as well as at Microsoft (2014, 2016) and EdgeCast Networks (2013). The routing testbed [73] led by PIs Katz-Bassett and Cunha, partially funded and developed as part of this grant, has been used in 8 papers [4, 76, 38, 61, 43, 81, 47, 77]. The PIs co-organized a BGP Hackathon in which 90 participants formed teams to conduct routing projects, including using the testbed. As part of the project, the PI organized preview sessions at SIGCOMM 2015 and SIGCOMM 2016 to provide junior members of the community with background to better understand the technical presentations. Each session had 80+ attendees, and we published a paper to encourage the practice in other communities [48]. The PI initiated and led the effort to improve the SIGCOMM anti-harassment policy to encourage a welcoming and diverse community. SIGCOMM conferences have adopted the policy, and it has been presented to other SIGs.

FL Nº 28
PROPP

Table 1: Planned tasks, participating institutions, and effort allocation.

Task	Lead	Effort Timeline Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
1. Tracking adoption of ROV (§2.1)									
1.1 Basic approach	Columbia								
1.2 Relax `visibility-assumption`	Columbia								
1.3 Relax `connected-assumption`	UFMG								
1.4 Evaluation	Columbia								
1.5 Longitudinal study	Columbia								
2. Locating origins of spoofed traffic (§2.2)									
2.1 Announcement manipulation tools	UFMG								
2.2 Integrate routing/topology metadata	Columbia								
2.3 Improve precision	UFMG								
2.4 Improve speed	UFMG								
2.5 Evaluation	UFMG								
3. Add security-specific functionality (§3.1)									
3.1 Originate spoofed traffic	UFMG								
3.2 ROA integration	Columbia								
3.3 Integration with DETER	Columbia†								
4. Support host/middlebox functionality (§3.2)									
4.1 On-router processing	UFMS								
4.2 Dysco support	UFMS								
4.3 Packet timing measurements	UFMS								
4.4 IPSec support	UFMG								
5. Enhance general functionality (§3.3)									
5.1 PEERING expansion	Columbia, UFMS*								
5.2 Experiment deployment	UFMG								
5.3 Route visibility	UFMG								
5.4 Route monitoring	UFMG								

† PI Katz-Bassett was with USC, which operates one DETER site.

* UFMS will lead expansion in South America.

computer science graduate programs at UFMG and UFMS have a bidirectional student and class exchange program. Ronaldo Ferreira recently finished a sabbatical at Princeton University and collaborates with Jennifer Rexford, who PI Katz-Bassett has also previously collaborated with.

Travel. The PIs attend the same conferences–SIGCOMM, IMC, etc.–every year, and end up meeting multiple times a year across these venues. We will leverage these in-person meeting opportunities to make long-term research plans. To strengthen collaboration and pursue research goals, this project plans 2 one-week trips for PI Katz-Bassett and one Ph.D. student to visit UFMG, as well as 6 one-month trips for Brazilian researchers and Ph.D. students to visit American universities. These extended trips will immerse Brazilian researchers and Ph.D. students in leading research groups in the US. Candidate dates for these trips include weeks preceding conference submission deadlines or adjacent to conferences. PI Katz-Bassett and PI Cunha have found these extended visits effective in the past.

Tasks, leaders, and effort allocation. Table 1 enumerates planned tasks. PIs Katz-Bassett and Cunha, along with their teams at Columbia and UFMG, will participate in all tasks. Co-PI Ferreira and his team at UFMS will lead the effort to support on-router functionality, NFV chaining, and timing measurements on the PEERING platform. The table shows an effort timeline, with darker shades meaning more effort. Tasks 3.2, 5.3, and 5.4 are prerequisites for tasks 1 and 2 and will be worked on first. Overall, we concentrate PEERING extension tasks in the beginning of the project to make new functionality available as soon as possible. We expect the timeline to be reasonably accurate for the first year but possibly different in the subsequent year. The proposed work is substantial, and the schedule aggressive, but we believe it is reasonable given our track record of collaboration.

FL Nº 29
PROPP

References

[1] https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/ (Cited on page 5).

[2] https://www.cloudflare.com/ddos/ (Cited on pages 5 and 8).

[3] Zahaib Akhtar, Alefiya Hussain, Ethan Katz-Bassett, and Ramesh Govindan. "DBit: Assessing Statistically Significant Differences in CDN Performance". In: *Computer Networks* 107 (1 2016), pp. 94–103 (Cited on page 8).

[4] R. Anwar, H. Niaz, D. R. Choffnes, Í. Cunha, P. Gill, and E. Katz-Bassett. "Investigating Interdomain Routing Policies in the Wild". In: *Proc. ACM IMC*. 2015 (Cited on pages 3, 4, 5, 6, 8, and 1).

[5] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies". In: *IEEE Symposium on Security and Privacy (to appear)*. 2017 (Cited on page 1).

[6] Hitesh Ballani, Paul Francis, and Xinyang Zhang. "A Study of Prefix Hijacking and Interception in the Internet". In: *Proc. ACM SIGCOMM*. 2007 (Cited on page 1).

[7] Robert Beverly, Arthur Berger, Young Hyun, and k claffy. "Understanding the Efficacy of Deployed Internet Source Address Validation Filtering". In: *Proc. ACM IMC*. 2009 (Cited on pages 1, 3, 5, and 6).

[8] R. Bush, O. Maennel, M. Roughan, and S. Uhlig. "Internet Optometry: Assessing the Broken Glasses in Internet Reachability". In: *Proc. ACM IMC*. 2009 (Cited on pages 3 and 5).

[9] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford. "A Survey of BGP Security Issues and Solutions". In: *Proceedings of the IEEE* 98.1 (2010), pp. 100–122 (Cited on page 8).

[10] M. Calder, X. Fan, Z. Hu, E. Katz-Bassett, J. Heidemann, and R. Govindan. "Mapping the Expansion of Google's Serving Infrastructure". In: *Proc. ACM IMC*. 2013 (Cited on pages 2 and 8).

[11] Matt Calder, Ashley Flavel, Ethan Katz-Bassett, Ratul Mahajan, and Jitendra Padhye. "Analyzing the Performance of an Anycast CDN". In: *Proc. ACM IMC*. 2015 (Cited on pages 2 and 8).

[12] Yi-Ching Chiu, Brandon Schlinker, Abhishek Balaji Radhakrishnan, Ethan Katz-Bassett, and Ramesh Govindan. "Are We One Hop Away from a Better Internet?" In: *Proc. ACM IMC*. 2015 (Cited on pages 3 and 8).

[13] Avichai Cohen, Yossi Gilad, Amir Herzberg, and Michael Schapira. "Jumpstarting BGP Security with Path-End Validation". In: *Proc. ACM SIGCOMM*. 2016 (Cited on page 8).

[14] L. Colitti. *Internet Topology Discovery Using Active Probing*. 2006 (Cited on page 3).

[15] Í. Cunha, R. Teixeira, and C. Diot. "Measuring and Characterizing End-to-End Route Dynamics in the Presence of Load Balancing". In: *Proc. PAM*. 2011 (Cited on page 3).

[16] Í. Cunha, R. Teixeira, N. Feamster, and C. Diot. "Measurement Methods for Fast and Accurate Blackhole Identification with Binary Tomography". In: *Proc. ACM IMC*. 2009 (Cited on page 3).

[17] Í Cunha, R. Teixeira, D. Veitch, and C. Diot. "DTRACK: A System to Predict and Track Internet Path Changes". In: *IEEE/ACM Trans. Netw.* 22.4 (2014), pp. 1025–1038 (Cited on pages 1 and 3).

[18] Í Cunha, Renata Teixeira, Nick Feamster, and Christophe Diot. "Distinguishing Persistent Failures from Transient Losses". In: *Proc. of ACM CoNEXT Student Workshop*. Madrid, Spain, 2008 (Cited on page 3).

[19] Italo Cunha, Pietro Marchetta, Matt Calder, Yi-Ching Chiu, Brandon Schlinker, Bruno V. A. Machado, Antonio Pescape, Vasileios Giotsas, Harsha V. Madhyastha, and Ethan Katz-Bassett. "Sibyl: A Practical Internet Route Oracle". In: *Proc. USENIX NSDI*. 2016 (Cited on pages 3, 8, and 1).

[20] Jakub Czyz, Michael Kallitsis, Manaf Gharaibeh, Christos Papadopoulos, Michael Bailey, and Manish Karir. "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks". In: *Proc. ACM IMC*. 2014 (Cited on page 5).

[21] Gessé Dafé, Adriano Veloso, Mohammed Zaki, and Wagner Meira Jr. "Learning Sequential Classifiers from Long and Noisy Discrete-event Sequences Efficiently". In: *Data Min. Knowl. Discov.* 29.6 (2015) (Cited on page 3).

Fl. Nº 20
PROPP

[41] Zi Hu, Liang Zhu, Calvin Ardi, Ethan Katz-Bassett, Harsha V. Madhyastha, John Heidemann, and Minlan Yu. "The Need for End-to-End Evaluation of Cloud Availability". In: *Proc. PAM*. 2014 (Cited on page 8).

[42] Daniele Iamartino, Cristel Pelsser, and Randy Bush. "Measuring BGP Route Origin Registration and Validation". In: *Proc. PAM*. 2015 (Cited on page 8).

[43] U. Javed, Í. Cunha, D. R. Choffnes, E. Katz-Bassett, T. Anderson, and A. Krishnamurthy. "PoiRoot: Investigating the Root Cause of Interdomain Path Changes". In: *Proc. ACM SIGCOMM*. 2013 (Cited on pages 3, 5, 6, 7, 8, and 1).

[44] J. P. John, E. Katz-Bassett, A. Krishnamurthy, T. Anderson, and A. Venkataramani. "Consensus Routing: the Internet as a Distributed System". In: *Proc. USENIX NSDI*. 2008 (Cited on page 3).

[45] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherry, P. van Wesep, A. Krishnamurthy, and T. Anderson. "Reverse Traceroute". In: *Proc. USENIX NSDI*. 2010 (Cited on pages 3, 5, 7, and 1).

[46] E. Katz-Bassett, H. Madhyastha, J. P. John, A. Krishnamurthy, D. Wetherall, and T. Anderson. "Studying Black Holes in the Internet with Hubble". In: *Proc. USENIX NSDI*. 2008 (Cited on pages 3 and 7).

[47] E. Katz-Bassett, C. Scott, D. R. Choffnes, Í. Cunha, V. Valancius, N. Feamster, H. V. Madhyastha, T. Anderson, and A. Krishnamurthy. "LIFEGUARD: Practical Repair of Persistent Route Failures". In: *Proc. ACM SIGCOMM*. 2012 (Cited on pages 3, 6, 7, 8, and 1).

[48] Ethan Katz-Bassett, Justine Sherry, Te-Yuan Huang, Maria Kazandjieva, Craig Partridge, and Fahad Dogar. "Helping Conference Attendees Better Understand Research Presentations". In: *Communications of the ACM* 59.9 (2016), pp. 32–34 (Cited on page 8).

[49] S. Kent, C. Lynn, and K. Seo. "Secure Border Gateway Protocol (S-BGP)". In: *IEEE J. Selected Areas in Communications* 18.4 (2006) (Cited on page 8).

[50] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian. "Delayed Internet Routing Convergence". In: *IEEE/ACM Trans. Netw.* 9.3 (2001), pp. 293–306 (Cited on page 6).

[51] *Level3 – DDoS Protection*. http://www.level3.com/en/products/ddos-mitigation/ (Cited on page 8).

[52] Matthew Luckie. "Scamper: A Scalable and Extensible Packet Prober for Active Measurement of the Internet". In: *Proc. ACM IMC*. 2010 (Cited on page 1).

[53] R. Mahajan, D. Wetherall, and T. Anderson. "Understanding BGP Misconfiguration". In: *Proc. ACM SIGCOMM*. 2002 (Cited on page 8).

[54] Z. M. Mao, R. Bush, T. G. Griffin, and M. Roughan. "BGP Beacons". In: *Proc. ACM IMC*. 2003 (Cited on page 3).

[55] J. Mirkovic, T. V. Benzel, T. Faber, R. Braden, J. T. Wroclawski, and S. Schwab. "The DETER project: Advancing the Science of Cyber Security Experimentation and Test". In: *Proc. IEEE Intl. Conf. on Technologies for Homeland Security (HST)*. 2010 (Cited on page 7).

[56] W. Mühlbauer, A. Feldmann, O. Maennel, M. Roughan, and S. Uhlig. "Building an AS-topology Model That Captures Route Diversity". In: *Proc. ACM SIGCOMM*. 2006 (Cited on page 1).

[57] *Network Functions Virtualization: An Introduction, Benefits, Enables, Challenges, and Call for Action*. 2012 (Cited on page 7).

[58] Ricardo V. Oliveira, Dan Pei, Walter Willinger, Beichuan Zhang, and Lixia Zhang. "In Search of the Elusive Ground Truth: The Internet's As-level Connectivity Structure". In: *Proc. ACM SIGMETRICS*. 2008 (Cited on page 1).

[59] Aurojit Panda, Sangjin Han, Keon Jang, Melvin Walls, Sylvia Ratnasamy, and Scott Shenker. "NetBricks: Taking the V out of NFV". In: *Proc. USENIX OSDI*. 2016 (Cited on pages 2 and 7).

[60] Vern Paxson. "An Analysis of Using Reflectors for Distributed Denial-of-service Attacks". In: *SIGCOMM Comput. Commun. Rev.* 31.3 (2001), pp. 38–47 (Cited on pages 1 and 5).

[61] S. Peter, U. Javed, Q. Zhang, D. Woos, A. Krishnamurthy, and T. Anderson. "One Tunnel is (Often) Enough". In: *Proc. ACM SIGCOMM*. 2014 (Cited on pages 3 and 8).

FL Nº 31
PROPP

[85] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, and D. Massey. "BGPmon: A Real-Time, Scalable, Extensible Monitoring System". In: *Proc. CATCH*. 2009 (Cited on pages 7 and 1).

[86] Mohammed J. Zaki and Wagner Meira Jr. *Data Mining and Analysis: Fundamental Concepts and Algorithms*. Cambridge University Press, 2014 (Cited on page 3).

[87] K. Zarifis, T. Flach, S. Nori, D. Choffnes, R. Govindan, E. Katz-Bassett, Z. M. Mao, and M. Welsh. "Diagnosing Path Inflation of Mobile Client Traffic". In: *Proc. PAM*. 2014 (Cited on pages 2 and 8).

[88] Kyriakos Zarifis, Mark Holland, Manish Jain, Ethan Katz-Bassett, and Ramesh Govindan. "Modeling HTTP/2 Speed from HTTP/1 Traces". In: *Proc. PAM*. 2016 (Cited on pages 3 and 8).

[89] Pamela Zave, Ronaldo A. Ferreira, Masaharu Morimoto, Xuan Zhou, and Jennifer Rexford. "Dynamic Service Chaining with Dysco (submitted)". In: *Proc. ACM SIGCOMM*. 2017 (Cited on pages 3 and 7).

FL Nº 32
PROPP

I am familiar with the PIs, their previous work in this area, and the plan in the current proposal, and I strongly believe that the PIs possess the expertise necessary to produce a successful result. As a researcher with expertise in Internet routing, measurement, and security, I believe that the proposed testbed functionality will be useful to the community at large. The PEERING testbed opens access to new routing and Internet security experiments.

Several of us at CAIDA are excited about the opportunity to continue working with the PIs and about the capabilities they propose for this project.

Sincerely,

Kimberly C. Claffy
Principal Investigator
Cooperative Association for Internet Data Analysis (CAIDA)
San Diego Supercomputer Center
UC San Diego
kc@caida.org
858-534-8333

FL Nº 33
E
PROPP

USC University of Southern California

INFORMATION SCIENCES INSTITUTE
Divisions
Advanced Electronics
Computational Systems and Technology
Informatics
Intelligent Systems

March 13, 2017

To whom it may concern:

I am the Project Leader at the USC Information Sciences Institute (ISI) and research faculty at USC. One of the projects I work on is DeterLab, a community cybersecurity testbed that has received funding from NSF, DHS, and DARPA. DETERLab provides a realistic, large-scale test environment for rigorous, repeatable cybersecurity experimentation.

I am writing in support of Ethan Katz-Bassett and Italo Cunha's proposal on in-the-wild Internet routing security research for the US-Brazil Collaboration on Cybersecurity Research. Specifically, this letter will describe our planned collaboration to federate DETERLab with their PEERING testbed. This federated testbed, along with the new PEERING functionality described in their proposal, will be useful in my own Internet security research, described below.

The two testbeds provide distinct, complementary functionality, and so federating them will enable experiments impossible with either one on its own. DETERLab provides a large number of computers to enable experiments at realistic scales, the ability to run malicious software in a safe environment, and other functionality designed for repeatable security research. However, although DETERLab has multiple sites, it does not give researchers the ability to control routing between them or between DETERLab sites and the Internet. This functionality is exactly what PEERING provides. A federation of the two testbeds will provide a novel environment for research on Internet-based attacks and defenses that exploit or rely on some element of routing. Examples of these are BGP prefix hijacking attacks and DDoS attacks. Both the attackers and the infrastructure/service could be run in DETERLab. I and others from the DETERLab will work with PIs Katz-Bassett and Cunha to enable experiments that use both testbeds, including easy deployment of resources that span both.

As a test case, I look forward to using the federated testbeds for my own SENSS project. SENSS is an interface that lets victim networks diagnose and mitigate attacks against them, via SENSS-based requests to other networks to provide measurements or install filters. An important goal of this DHS-funded research is a deployable prototype and outreach to the network operations community. We can use PEERING both to emulate attacks and then to demonstrate the ability of SENSS to diagnose and mitigate them. These experiments will require new PEERING functionality that PI Katz-Bassett and Cunha are proposing, including federation with DETERLab, controlled spoofing, and NFV support (to deploy SENSS at PEERING routers).

Once we establish the federation, other researchers will be able to jointly use DETERLab and PEERING in their own research, expanding the impact of both testbeds.

I hope NSF and RNP/CTIC fund this proposal so that I can work with the PIs on this federated infrastructure and use it in my own research. I am familiar with previous research from both PIs and think their expertise will enable exciting results at the intersection of Internet routing and cybersecurity.

Jelena Mirkovic
Research Assistant Professor
USC Information Sciences Institute
4676 Admiralty Way, Suite 1001
Marina del Rey, CA 90292
310-448-9170

Fl. Nº 34
PROPP

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Computer Engineering and
Networks Laboratory

Prof. Dr. Laurent Vanbever

ETH Zurich
ETZ G 90
Gloriastrasse 35
8092 Zurich, Switzerland

Phone +41 44 632 70 04
Fax +41 44 632 10 36
Mobile +41 79 604 56 14
lvanbever@ethz.ch
www.vanbever.eu

Zurich, March 16, 2017

Object: Recommendation letter for Mr. Ethan Katz-Bassett and Mr. Ítalo Cunha

To whom it may concern,

I am writing to express my interest in collaborating with Ethan Katz-Bassett and Italo Cunha on the work described in their proposal "Researching Internet Routing Security in the Wild". I am an assistant professor at ETH Zürich, and much of my interest focuses on Internet routing.

As increasingly important services run on the Internet, Internet routing is a critical component of cybersecurity. My research has looked at how routing can be used to attack systems including Bitcoin and Tor. I have also investigated how networks can prevent traffic analysis, how networks can delegate control to others, and how routers can "lie" to induce desired outcomes. We need research to understand the vulnerabilities of the Internet and of systems that run on it, and to design protections. To conduct this research, researchers need effective means to measure the Internet and to prototype and evaluate their solutions.

The work in this proposal will make PI Katz-Bassett and Cunha's PEERING testbed a great resource for Internet security research. With students and collaborators, I have used the testbed in 4 publications, on Software-Defined Internet Exchanges (SIGCOMM 2014), inbound traffic engineering (SOSR 2015), routing attacks on Tor (USENIX Security Symposium 2015), and routing attacks on Bitcoin (IEEE Symposium on Security and Privacy 2017). In the last paper, for example, we used the testbed to measure the time it takes for an attacker to divert traffic after a route hijack. When we previously submitted this paper without this evaluation, the peer reviewers did not believe some of the claims in the paper, and so it was rejected. PEERING let us demonstrate the attack in the wild, with real measurements of its effectiveness. These experiments helped convince reviewers at the prestigious IEEE S&P conference to accept the paper.

I look forward to helping the PIs design the new functionality described in the proposal then using it in my research. Features such as the ability to support host and middlebox functionality on PEERING routers and the ability to issue Route Origin Authorizations for PEERING prefixes will enable new experiments on Internet security, including on defenses against the types of attacks my previous work demonstrated.

In addition to using PEERING in my research, I look forward to continuing to collaborate with the PIs on two other aspects of the work. First, one of my students attended the BGP hackathon co-organized by PIs Katz-Bassett and Cunha. This event introduced my student to PEERING and to researchers and operators interested in similar problems. Second, I have used PEERING's emulation environment as the basis for a class project in which each student configures their own network, then interconnects with other students' networks and configures the routing policies that encode business relationships and determine routing on today's Internet. This exercise gives students hands-on experience and reinforces material from class. I shared this project with PI Katz-Bassett,

Fl. Nº 35
PROPP

Freie Universität Berlin

Department of Mathematics and Computer Science
Institute of Computer Science

Freie Universität Berlin, Fachbereich Mathematik und Informatik
Takustr. 9, 14195 Berlin, Germany

Prof. Dr. Matthias Wählisch
Takustr. 9
14195 Berlin, Germany

Telephone +49 30 838-50072
Fax +49 30 838-4 50072
E-Mail m.waehlisch@fu-berlin.de
Internet http://www.cs.fu-berlin.de/~waehl

Berlin, March 13, 2017

Collaboration letter for Prof. Katz Bassett and Prof. Cunha

To whom it may concern:

I write this letter to describe my collaboration with Ethan Katz-Bassett and Italo Cunha as well as to express my interest in the research described in their proposal on Internet routing security for the US-Brazil Collaboration on Cybersecurity Research.

I am an Assistant Professor of Computer Science at Freie Universität Berlin. Much of my research is on Internet security: I organize recurring Dagstuhl Seminars on "The Critical Internet Infrastructure," I am the PI of several cybersecurity projects funded in the Federal Cybersecurity Research Program by the German Government, and I regularly participate in and present on routing security at IETF and NANOG meetings.

I collaborate with Profs. Katz-Bassett and Cunha on a characterization of RPKI deployment in the Internet. In the first component of the work, we demonstrated that uncontrolled experiments that rely on passive measurement of existing Internet routes (such as the experiments described in a recent NDSS 2017 paper) can lead to false inferences. This result demonstrates the need for controlled experiments that actively manipulate routes, as can be enabled with the PEERING testbed. In our collaboration, we are beginning to use the PEERING testbed to conduct active measurements of interdomain routes under different RPKI validation states, as described in the proposal. Without access to PEERING routers at multiple locations, we would have been forced to conduct the study with much less peering connectivity and Internet coverage, and this type of research would be off-limits to most researchers entirely, as they lack the Internet resources.

The proposed extensions to improve route visibility and monitoring will benefit our study, reducing the amount of manual investigation we need to perform to interpret the observations. The proposed extensions to integrate PEERING prefixes with the RPKI and to announce our own prefixes through PEERING routers will ease the setup process for studies such as ours going forward. I believe the proposed extensions will ease the deployment, data collection, and analysis of future security-related experiments.

Fl. Nº 36
PROPP

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Amsterdam, 15 March 2017

To whom it may concern:

I am writing to support the proposal by Profs. Cunha and Katz-Bassett's on expanding the PEERING research testbed and studying routing and forwarding security issues in the Internet, as well as to describe the RIPE NCC's ongoing collaboration with this team. The RIPE NCC is Europe's not-for-profit membership organisation that supports the infrastructure of the Internet through technical coordination in our service region. I am Manager of the Research and Development department at the RIPE NCC. I lead a dedicated team of thinkers to support the RIPE community by providing network research, data analysis and prototype tool development.

The RIPE NCC has previously collaborated with Profs. Cunha and Katz-Bassett in enabling high-coverage measurements from RIPE Atlas, our platform of over 9000 measurement vantage points distributed around the world. We coordinated with the PIs on measurement configuration to avoid overloading destinations. The RIPE NCC currently supports the PEERING testbed by issuing ongoing traceroute measurements from RIPE Atlas toward PEERING prefixes. We support the proposed work on expanding route visibility to PEERING prefixes and are working with Profs. Cunha and Katz-Bassett to increase the flexibility and frequency of measurements to PEERING prefixes, by, e.g., configuring measurements to target a PEERING-controlled DNS name and hosting a second RIPE Atlas Anchor in Brazil at UFMG. We also provide the RIPE Routing Information Service (RIS), which provides routing information from many networks towards Internet destinations, including PEERING destinations. We also helped co-organize and participated in the first BGP hackathon with the PIs. The hackathon introduced 90 participants to Internet routing tools including RIPE RIS and PEERING. We look forward to similar events in the future.

We also believe the proposed research on characterizing RPKI Route Origin Authorization (ROA) filtering and locating spoofed traffic is of interest to RIPE NCC members and the network operator community in general. We have previously hosted PI Katz-Bassett to speak about his research to network operators at RIPE meetings, and we look forward to helping the PIs present their proposed Internet security work to the community in the future.

We hope that NSF/RNP will fund this proposal. We look forward to continuing to work with Profs. Cunha and Katz-Bassett on expanding monitoring toward PEERING prefixes to support their proposed research.

Yours sincerely,

Robert Kisteleki
Manager Research&Development
RIPE NCC

Stationsplein 11
P.O. Box 10096
1001 EB Amsterdam
The Netherlands

T: +31 20 535 4444
F: +31 20 535 4445
E: ncc@ripe.net
W: www.ripe.net

FL Nº 37
PROPP

2. Coordinated the United Nations' IGF Best Practices Forums on "Countering Spam" and on "Computer Security Incident Response Teams for Internet Security", 2014, 2015.
3. Member of the Forum of Incident Response and Security Teams (FIRST) Board of Directors, 2012, 2013.
4. Member of the Experts Group of the FIRST Education Program, that has developed the Security Incident Response Teams Services Framework, upon which an educational curriculum for Incident Handling professionals will be built.

FL Nº 38
8
PROPP

Synergistic Activities

1. Technical Program Committee Member for ACM SIGCOMM 2017; ACM IMC 2016; ACM CoNEXT 2015, 2016; Passive and Active Measurements Conference (PAM) 2013, 2015; IFIP Networking 2013, 2014, 2015, 2016; Traffic Monitoring and Analysis (TMA) 2013, 2014, 2015, 2016. Member of the RNP Network Monitoring Working Group (CT-MON).
2. Contributor to the *PEERING* BGP community testbed. Presented and demonstrated *PEERING* at Brazilian conferences and universities.
3. Co-organized BGP routing hackathon, bringing together 80 participants from academia, industry, and network operations to learn about available routing tools and testbests (including *PEERING*) and to work together on research and development projects.

Fl. Nº 29
PROPP

4. "A Campaign-based Characterization of Spamming Strategies." P. Calais, D. E. V. Pires, D. Guedes, W. Meira Jr., C. Hoepers, K. Steding-Jessen. *Conference on Email and Anti-Spam (CEAS)*, 2008.
5. "Anteater: A Service-oriented Architecture for High-performance Data Mining." D. Guedes, W. Meira Jr., R. Ferreira. *IEEE Internet computing* 10(4), 2006.

Synergistic Activities

1. Coordinator of the Special Interest Groups in Computer Networks and Distributed Systems of the Brazilian Computer Society (SBC), 2013–2015.
2. Member of the Administrative Board of the Brazilian Academic Research Network (RNP), 2013–2015.

FL. Nº 40
PROPP

4. "iPlane Nano: Path Prediction for Peer-to-Peer Applications." H. V. Madhyastha, E. Katz-Bassett, T. Anderson, A. Krishnamurthy, A. Venkataramani. *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2009.
5. "Consensus Routing: The Internet as a Distributed System." J. P. John, E. Katz-Bassett, A. Krishnamurthy, T. Anderson, A. Venkataramani. *USENIX Symposium on Networked Systems Design & Implementation (NSDI)*, 2008. **Awarded Best Paper.**

Synergistic Activities

1. Technical Program Committee Member for ACM SIGCOMM 2014, 2015, 2016; USENIX Symposium on Networked Systems Design & Implementation (NSDI) 2013, 2014, 2015; Internet Measurement Conference (IMC) 2013, 2015, 2016, 2017; Passive and Active Measurements Conference (PAM) 2015; ACM MobiSys (external review committee) 2014.
2. Lead PI for *PEERING* BGP community testbed, which since 2011 has been used for 4 SIGCOMM papers, 1 SIGMETRICS paper, 1 IMC paper, 1 HotNets paper, 1 SOSR paper, and 1 USENIX Security paper.
3. Co-organized BGP routing hackathon, bringing together 80 participants from academia, industry, and network operations to learn about available routing tools and testbests (including *PEERING*) and to work together on research and development projects. CCR article published in 2016 describing the hackathon.
4. Presented multiple times on routing and Internet measurement to network operator audiences, including at NANOG, RIPE (invited speaker), and RAIM (invited keynote). Collaborate with Microsoft and Facebook on controlling aspects of their Internet routing.
5. Proposed and organized background sessions at SIGCOMM 2014, 2015, and 2016 to make technical talks more accessible, especially to newcomers to SIGCOMM. Ran small-scale 2014 version as part of N2Women mentoring program for women. Ran larger verison in 2015 with 80 attendees per session. CACM paper published in 2016 describing the sessions. Currently organizing 2017 version.

FL Nº 41
PROPP

honeypots hosted at partner organizations from academia, government, private and critical infrastructure sectors. Since 2007 there is also a global network of sensors, called SpamPots Project, that focus in collecting data related to the abuse of the Internet infrastructure by spammers. The SpamPots Project has as partners CERTs, universities and not for profit organizations from 14 countries.

2. Leads the CERT.br information sharing efforts, that encompass the identification and sharing of indicators of compromise, including data from the honeyTARG Project, with community organizations such as Team Cymru, CyberGreen and ShadowServer.
3. Technical Program Committee Member for the Annual FIRST Conference on Computer Security Incident Handling 2006.

Fl. Nº 42
PROPP

Other Significant Publications

1. "Learning Sequential Classifiers from Long and Noisy Discrete-event Sequences Efficiently" G. Daf, A. Veloso, M. Zaki, W. Meira Jr. *Data Mining and Knowledge Discovery,* 29(6), 1685–1708, 2015.
2. "Data Mining and Analysis: Fundamental Concepts and Algorithms." M. J. Zaki and W. Meira Jr. *Cambridge University Press,* 2014.
3. "Diagnosing Performance Bottlenecks in Massive Data Parallel Programs." V. Dias, R. Moreira, W. Meira Jr., D. Guedes. *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, 2016.
4. "Is there a Best Quality Metric for Graph Clusters?" H. Almeida, D. Guedes, W. Meira Jr., M. J. Zaki. *Joint European Conf. on Machine Learning and Knowledge Discovery in Databases*, 2011.
5. "Anteater: A Service-oriented Architecture for High-performance Data Mining." D. Guedes, W. Meira Jr., R. Ferreira. *IEEE Internet computing,* 10(4), 2006.

Synergistic Activities

1. Member of the advisory board of the Brazilian Computer Society (SBC), National Agency for Scientific and Technological Development (CNPq), and Minas Gerais State Research Foundation (FAPEMIG).
2. Program director, SIAM Activity Group on Data Mining and Analytics (SIAGDMA), 2016-2017.
3. Editorial Board, Data Mining and Knowledge Discovery, Springer.
4. Computer Science graduate program coordinator at UFMG from 2009 to 2014.
5. Participated in the organization committees of 12 conferences and workshops.

Fl. Nº 43
PROPP

3. R. A. Ferreira, M. K. Ramanathan, A. Grama, and S. Jagannathan. Randomized Protocols for Duplicate Elimination in Peer-to-Peer Storage Systems. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, Volume 18, Number 5, pages 686–696, May 2007.
4. M. K. Ramanathan, R. A. Ferreira, S. Jagannathan, A. Grama, and W. Szpankowski. Randomized Leader Election. *Distributed Computing*, Volume 19, Number 5-6, pages 403–418, April 2007.
5. R. A. Ferreira, M. K. Ramanathan, A. Awan, A. Grama, and S. Jagannathan. Search with Probabilistic Guarantees in Unstructured Peer-to-Peer Networks. *The 5th IEEE International Conference on Peer-to-Peer Computing (P2P 2005)*, pages 165–172, August 2005.

Synergistic Activities

1. Co-organized the Brazilian workshop Grand Research Challenges in Computer Networks and Distributed Systems in 2013 that brought together a group of 28 researchers to identify and define an agenda for the research challenges in computer networks and distributed systems for the next ten years.
2. Chaired the Special Interest Group in Computer Networks and Distributed Systems of the Brazilian Computer Society from 2011 to 2013.
3. Involvement in scientific conferences: publicity chair of SIGCOMM 2016, general chair of the Brazilian Symposium on Computer Networks and Distributed Systems 2011 (SBRC'11), TCP Co-Chair of the IFIP/ACM Latin American Networking Conference 2012 (LANC'12).
4. Coordinated the construction of a metropolitan network that connects the education and research institutions of the city of Campo Grande and serves as an IXP.
5. Co-coordinated the development of the technology and tools used by the Brazilian universities to access the Eduroam authentication service.

Fl. Nº 44
PROPP

Ítalo Cunha (Collaborators)
Assistant Professor, Department of Computer Science
Universidade Federal de Minas Gerais, Brazil
cunha@dcc.ufmg.br

Collaborators and Other Affiliations

- **External Collaborators:** Randy Bush (IIJ), David R. Choffnes (Northeastern University), Christophe Diot (Safran), Phillipa Gill (Stony Brook University), Vasilis Giotsas (UCSD/CAIDA), Harsha V. Madhyastha (Michigan), Antonio Pescapè (University of Napoli Federico II), Renata Teixeira (INRIA), Darryl Veitch (University of Technology Sydney), Matthias Waehlisch (FU-Berlin).
- **Graduate Advisors:** Christophe Diot (Safran), Renata Teixeira (INRIA).
- **Ph.D. Students:** Elverton Fazzion.

Fl. Nº 45
PROPP

Ethan Katz-Bassett (Collaborators)
Assistant Professor, Department of Computer Science
University of Southern California
Starting summer 2017:
Associate Professor without tenure, Department of Electrical Engineering
Columbia University
ethan.kb@usc.edu

Collaborators and Other Affiliations

- **E. Collaborators and Co-Editors:** Tom Anderson (University of Washington), Neal Cardwell (Google), Yuchung Cheng (Google), Marshini Chetty (University of Maryland), David Choffnes (Northeastern University), Russ Clark (Georgia Tech), Italo Cunha (UFMG), Nandita Dukkipati (Google), Nick Feamster (Princeton), Ashley Flavel (Salesforce), Phillipa Gill (Stony Brook University), Vasilis Giotsas (UCSD/CAIDA), Ramesh Govindan (USC), Shuai Hao (AT&T Research), John Heidemann (USC/ISI), Mark Holland (Akamai), Alifya Hussain (ISI), Ankur Jain (Google), Manish Jain (Akamai), Arash Kakhki (Northeastern University), Arvind Krishnamurthy (UW), Harsha V. Madhyastha (UCR), Ratul Mahajan (Microsoft Research), Z. Morley Mao (Michigan), Alan Mislove (Northeastern University), Jeffrey C. Mogul (Google), Radhika Niranjan Mysore (Google), Jitu Padhye (Microsoft Research), Pavlos Papageorge (Google), Antonio Pescape (University of Napoli Federico II), Barath Raghavan (ICSI), Jennifer Rexford (Princeton), Michael Rubin (Google), Scott Shenker (UC Berkeley), Sean Smith (Google), Colin Scott (UCB), Justine Sherry (UCB), Andreas Terzis (Google), Amin Vahdat (Google), Vytautas Valancius (Google), Laurent Vanbever (ETH Zurich), Matt Welsh (Google), Minlan Yu (USC)
- **Graduate Advisors:** Tom Anderson (University of Washington), Arvind Krishnamurthy (University of Washington)
- **PhD Advisor:** Matt Calder, Yi-Ching Chiu, Tobias Flach, Chris Hodsdon, Aqib Nisar, Brandon Schlinker, Theano Stavrinos, Kyriakos Zarifis.

Fl. Nº 46
PROPP

Wagner Meira Jr. (Collaborators)
Professor, Department of Computer Science
Universidade Federal de Minas Gerais, Brazil
meira@dcc.ufmg.br

Collaborators and Other Affiliations

- **Collaborators and co-Editors:** Ponnurangam Kumaraguru (Indraprastha Institute of Information Technology), Joel H. Saltz (Emory University), Mohammed J. Zaki (RPI).
- **Graduate Advisor:** Thomas John LeBlanc (University of Rochester).
- **PhD Advisor:** Eduardo M. P. Coelho, Bruno R. Coutinho, Felipe Ferré, Pedro H. C. Guerra, Elisa B. Lima, Raquel C. Melo, Fernando H. J. Mourão, Deive C. Oliveira, Rafael S. Oliveira, Adriano C. M. Pereira, Douglas E. V. Pires, Bruno A. V. Pôssas, Leonardo C. D. Rocha, Cristiano M. Silva, Carlos H. Silveira, Sabrina A. Silveira, Adriano A. Veloso, Caio J. M. Veloso, Renê R. Veloso.

FL Nº 417

RNP

CTIC

Rede Nacional de Ensino e Pesquisa - RNP
Chamada RNP-NSF em Segurança Cibernética
ANEXO II - Cronograma Físico-Financeiro

Researching Internet Routing Security in the Wild - UFMS

Duração do projeto: 24 meses

Resumo Físico-Financeiro por Prazo

ID dos produtos: Informar os produtos (*deliverables*) que serão entregues em cada trimestre conforme descrições nas tabelas seguintes. Ex. D1.1, D3.4, D2.5 e D1.5.
* As 'Despesas acessórias' relacionadas a equipamentos e softwares deverão ser somados e apresentados na coluna "Equipamentos".
** Os recursos para compra de equipamentos e softwares deverão ser informados, mas não entram no total, pois não serão repassados à contratada. Esses recursos serão mantidos na RNP que se responsabilizará pelas aquisições.

Prazo	ID dos produtos	Passagens / Diárias	Material permanente, bibliográfico, de consumo e despesas acessórias	Pessoal	Serviços de Terceiros	TOTAL	Equipamentos**
M00	----------	R$ 30.000,00	R$ 15.000,00	R$ 13.500,00	R$ 3.000,00	R$ 61.500,00	R$ 178.736,84
M03				R$ 13.500,00		R$ 13.500,00	R$ -
M06		R$ 30.000,00	R$ 5.000,00	R$ 24.300,00		R$ 59.300,00	R$ -
M09				R$ 24.300,00		R$ 24.300,00	R$ -
M12	D4.1, D4.2	R$ 20.000,00	R$ 5.000,00	R$ 24.300,00	R$ 1.700,00	R$ 51.000,00	R$ -
M15				R$ 24.300,00		R$ 24.300,00	R$ -
M18	D4.3, D4.4	R$ 13.704,00	R$ 3.702,32	R$ 13.500,00		R$ 30.906,32	R$ -
M21				R$ 13.500,00		R$ 13.500,00	R$ -
M24	D4.5, D4.6, D4.7, D5.1, D5.2	--	--	--	--	--	--
Total:		**R$ 93.704,00**	**R$ 28.702,32**	**R$ 151.200,00**	**R$ 4.700,00**	**R$ 278.306,32**	**R$ 178.736,84**

4. Produtos Finais do Módulo 4 (WP4): Support host/middlebox functionality

Responsável: Nome da instituição e do representante que responderá pelo Produto (formato: <SIGLA da instituição> : <Nome do representante>)
Tipos: São exemplos de tipo de produto o Relatório, Protótipo, Sistema e Equipamento
Data de entrega : A data de entrega deve ser informada em função do trimestre de entrega. Ex.: M3, M12, M18

ID	Descrição do Produto	Instituições envolvidas	Responsável	Tipo	Data de Entrega
D4.1	Suporte a NFV nos roteadores PEERING	UFMS	UFMS:Ronaldo Ferreira	Software	M12
D4.2	Documentação sobre o uso de NFV nos roteadores PEERING	UFMS	UFMS:Ronaldo Ferreira	Documentação	M12
D4.3	Suporte ao protocolo Dysco no PEERING	UFMS	UFMS:Ronaldo Ferreira	Software	M18
D4.4	Documentação sobre o uso de Dysco no PEERING	UFMS	UFMS:Ronaldo Ferreira	Documentação	M18
D4.5	Infraestrutura para medições de desempenho no PEERING	UFMS	UFMS:Ronaldo Ferreira	Software	M24
D4.6	Documentação sobre o uso da infraestrutura para medições de desempenho	UFMS	UFMS:Ronaldo Ferreira	Documentação	M24
D4.7	Artigo científico	UFMS	UFMS:Ronaldo Ferreira	Artigo	até M24

5. Produtos Finais do Módulo 5 (WP5): Enhance general functionality

Responsável: Nome da instituição e do representante que responderá pelo Produto (formato: <SIGLA da instituição> : <Nome do representante>)
Tipos: São exemplos de tipo de produto o Relatório, Protótipo, Sistema e Equipamento
Data de entrega : A data de entrega deve ser informada em função do trimestre de entrega. Ex.: M3, M12, M18

ID	Descrição do Produto	Instituições envolvidas	Responsável	Tipo	Data de Entrega
D5.1	Expansão do PEERING na UFMS	UFMS	UFMS:Ronaldo Ferreira	Hardware	até M24
D5.2	Expansão do PEERING em SP	UFMS, UFMG, Columbia, NIC.br	UFMS:Ronaldo Ferreira	Hardware	até M24

FL. Nº 48
PROC.

RNP

CTIC

Rede Nacional de Ensino e Pesquisa - RNP
Chamada RNP-NSF em Segurança Cibernética
Anexo III - Cronograma de Atividades

Researching Internet Routing Security in the Wild

	Lead	2017				2018												2019							
		9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8
Pacote de Trabalho WP1: Tracking adoption of ROV																									
Atividade 1.1: Basic approach	Columbia							■	■	■	■	■	■	■	■	■	■								
Atividade 1.2: Relax "visibility assumption"	Columbia									■	■	■	■	■	■	■	■	■	■						
Atividade 1.3: Relax "connected-assumption"	UFMG												■	■	■	■	■	■	■	■	■	■	■	■	■
Atividade 1.4: Evaluation	Columbia																			■	■	■	■	■	■
Atividade 1.5: Longitudinal study	Columbia										■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Pacote de Trabalho WP2: Locating origins of spoofed traffic																									
Atividade 2.1: Announcement manipulation tools	UFMG							■	■	■	■	■	■	■	■	■	■	■	■						
Atividade 2.2: Integrate routing/topology metadata	Columbia							■	■	■	■	■	■												
Atividade 2.3: Improve precision	UFMG										■	■	■	■	■	■	■	■	■	■	■	■	■		
Atividade 2.4: Improve speed	UFMG												■	■	■	■	■	■	■	■	■	■	■	■	■
Atividade 2.5: Evaluation	UFMG																■	■	■	■	■	■	■	■	■
Pacote de Trabalho WP3: Add security-specific functionality																									
Atividade 3.1: Originate spoofed traffic	UFMG												■	■	■	■	■	■	■						
Atividade 3.2: ROA integration	Columbia	■	■	■	■	■	■																		
Atividade 3.3: Integration with DETER	Columbia/USC	■	■	■	■	■	■	■	■	■	■	■	■												
Pacote de Trabalho WP4: Support host/middlebox functionality																									
Atividade 4.1: On-router processing	UFMS	■	■	■	■	■	■	■	■	■	■	■	■												
Atividade 4.2: Dysco support	UFMS							■	■	■	■	■	■	■	■	■	■	■	■						
Atividade 4.3: Packet timing measurements	UFMS																■	■	■	■	■	■	■	■	■
Atividade 4.4: IPSec support	UFMG																			■	■	■	■	■	■
Pacote de Trabalho WP5: Enhance general functionality																									
Atividade 5.1: PEERING expansion	Columbia/UFMS	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Atividade 5.2: Experiment deployment	UFMG	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■								
Atividade 5.3: Route visibility	UFMG	■	■	■	■	■	■																		
Atividade 5.4: Route monitoring	UFMG	■	■	■	■	■	■																		

Fl. Nº 49
PROPP

RNP

Rede Nacional de Ensino e Pesquisa - RNP
Chamada RNP-NSF em Segurança Cibernética
ANEXO IV - Orçamento Detalhado Definitivo

Researching Internet Routing Security in the Wild - UFMS

*** ID dos produtos:** Informar os IDs dos produtos/pacotes de trabalho que serão desenvolvidos com o uso do recurso especificado. Ex. D1.2, D3.2 e WP5

1. Viagens Nacionais/Internacionais

Passagens aéreas (nacionais e internacionais) e diárias devidamente adequadas a quaisquer dos seguintes objetivos:
1. Realização de reuniões do projeto;
2. Testes em outras regiões/laboratórios;
3. Visitas a fornecedores e parceiros de desenvolvimento; e
4. Participação em eventos científicos com apresentação de trabalho relacionado ao projeto.

ID dos produtos / pacote de trabalho	Especificação	Objetivo	Valor unitário	Qtd.	Valor total
Todos	Passagens	Colaboração	R$ 4.500,00	4	R$ 18.000,00
Todos	Diárias	Colaboração	R$ 1.147,00	46	R$ 52.762,00
D4.7/WP 4	Diárias para apresentação de artigo no exterior	Divulgação	R$ 1.147,00	6	R$ 6.882,00
D4.7/WP 4	Passagens para apresentação de artigo no exterior	Divulgação	R$ 4.500,00	1	R$ 4.500,00
Todos	Intercâmbio UFMS/UFMG	Colaboração	R$ 320,00	28	R$ 8.960,00
Todos	Intercâmbio UFMS/UFMG	Colaboração	R$ 1.300,00	2	R$ 2.600,00
TOTAL			R$ 12.914,00	87	R$ 93.704,00

2. Material permanente, bibliográfico, de consumo e despesas acessórias

Informar os recursos referentes aos seguintes itens financiáveis:
. Material permanente;
. Material de consumo, componentes e/ou peças de reposição de equipamentos, instalação, recuperação e manutenção de equipamentos, material de informática e componentes para montagem de protótipos e confecção de placas;
. Material bibliográfico; e
. Despesas acessórias, desde que não relacionadas aos equipamentos. As despesas acessórias relacionadas aos equipamentos deverão ser informadas no item "5. Equipamentos".

ID dos produtos / pacote de trabalho	Descrição	Instituição de destino	Valor unitário	Qtd.	Valor total
Todos	Material bibliográfico	UFMS	R$ 300,00	8	R$ 2.400,00
Todos	Material de escritório	UFMS	R$ 3.687,00	1	R$ 3.687,00
Todos	Peças de reposição	UFMS	R$ 7.000,00	1	R$ 7.000,00
Todos	Acessórios para teleconferências	UFMS	R$ 500,00	1	R$ 500,00
Todos	Despesas de instalação de equipamento	UFMS	R$ 1.200,00	1	R$ 1.200,00
Todos	*Custos Incorridos na Gestão do Projeto*	*FAPEC*	*R$ 13.915,32*	*1*	*R$ 13.915,32*
TOTAL			R$ 26.602,32		R$ 28.702,32

3. Pessoal

Descrever os perfis dos membros da equipe que participarão no projeto (não é necessário especificar os nomes, a não ser no caso de tarefas de coordenação).
Exemplos: Bolsa IC, Estagiário, Bolsa Mestrado, Gerente de Projetos CLT, Assistente Administrativo CLT, Bolsa DTI ...

ID dos produtos / pacote de trabalho	Especificação	Carga semanal (horas)	Nº de Meses	Valor mensal	Qtd.	Valor total
WP 4	Bolsa de Doutorado	40	18	R$ 3.600,00	1	R$ 64.800,00
WP 4	Bolsa de Doutorado	40	18	R$ 3.600,00	1	R$ 64.800,00
WP 4	Bolsa de Iniciação científica	20	24	R$ 900,00	1	R$ 21.600,00
TOTAL				R$ 8.100,00	3	R$ 151.200,00

4. Serviços Terceiros

Serviços de terceiros - pagamento integral ou parcial de contratos de manutenção e serviços de terceiros, pessoa física ou jurídica, de caráter eventual. Os recursos alocados para Inscrições em eventos deverão constar nesta lista.

ID dos produtos / pacote de trabalho	Especificação	Valor unitário	Qtd.	Valor total
D4.7/WP 4	Inscrição em conferência internacional	R$ 3.500,00	1	R$ 3.500,00
Todos	Computação em núvem	R$ 1.200,00	1	R$ 1.200,00
TOTAL		R$ 4.700,00	2	R$ 4.700,00

5. Equipamentos

Fl. Nº 50
6
PROPP

Os itens de capital serão alocados na instituição de execução do projeto sob a responsabilidade, manutenção e guarda do Coordenador/Instituição de execução do projeto.
Informar os equipamentos e softwares, além das despesas acessórias ligadas a eles, especialmente as de importação e as de instalações necessárias ao seu adequado funcionamento.
:: No caso das importações, recomenda-se que seja considerado um custo entre 10% e 15% do valor total do material a ser importado para cubrir despesas gerais (frete internacional, nacional, seguro, honorários de despachante, etc).
Os recursos para compra de equipamentos e softwares informados não serão repassados à contratada. Esses recursos serão mantidos na RNP que se responsabilizará pelas aquisições.

ID dos produtos / pacote de trabalho	Descrição	Data de início da utilização	Instituição de destino	Valor unitário	Qtd.	Valor total
D5.1	PEERING router	01/01/2018	UFMS	R$ 36.000,00	1	R$ 36.000,00
D5.2	PEERING router	01/01/2018	UFMS	R$ 36.000,00	1	R$ 36.000,00
Todos	Servidor de avaliação de rede	01/01/2018	UFMS	R$ 23.000,00	2	R$ 46.000,00
Todos	Estação de Trabalho/Notebook	01/01/2018	UFMS	R$ 12.000,00	3	R$ 36.000,00
Todos	No-break empilhável	01/01/2018	UFMS	R$ 5.000,00	1	R$ 5.000,00
Todos	Switch	01/01/2018	UFMS	R$ 19.736,84	1	R$ 19.736,84
TOTAL				R$ 131.736,84	9	R$ 178.736,84

TOTAL	R$	457.043,16