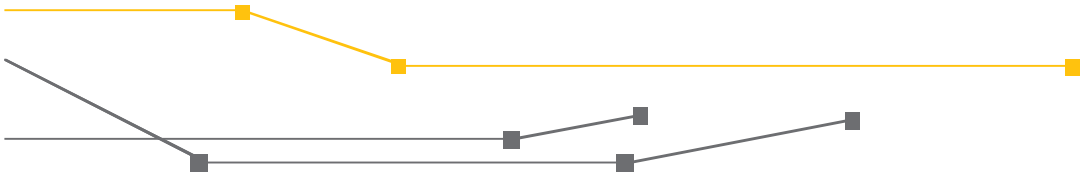
Chamada para apresentação de soluções para sigilo do fone@RNP

Carta-convite

RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CULTURA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES BRASIL GOVERNO FEDERAL



A Rede Nacional de Ensino e Pesquisa (RNP) quer melhorar a segurança do seu serviço de voz sobre IP fone@RNP, ao incorporar soluções de criptografia. Para isso, gostaria de contar com o conhecimento e a experiência da comunidade.

Este documento formaliza o convite a profissionais e suas instituições a apresentarem soluções que promovam sigilo para mídia e sinalização de uma rede de telefonia baseada em SIP (*Session Initiation Protocol*).

Motivação

O fone@RNP é seguro e conta com soluções como acesso autenticado para qualquer atividade, perfis diferenciados, logs de auditoria, *firewall* interno, só aceita convites de *peers* conhecidos. Entretanto, com relação ao sigilo das chamadas, o fone@RNP oferece segurança equivalente ao serviço tradicional de telefonia, ou seja, não há criptografia.

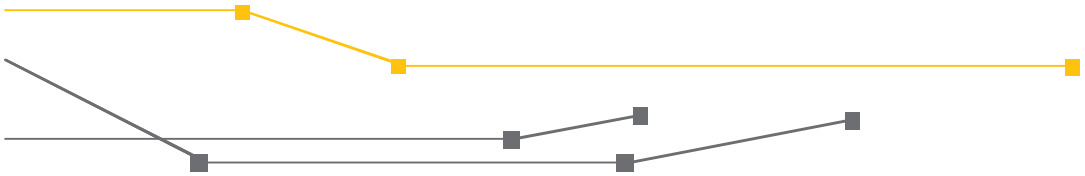
As informações sigilosas trazidas a público pelo ex-agente da CIA Edward Snowden lançaram preocupações no governo brasileiro, que desencadearam uma série de ações para melhorar a segurança da informação no país. Uma das iniciativas foi a publicação do Decreto-Lei 8135, de 4 de novembro de 2013, que exige medidas de instituições nacionais para manter o sigilo das informações.

Nesse contexto, cresceram também as preocupações com as informações sobre os estudos realizados em universidades e unidades de pesquisa. Boa parte dessas instituições é cliente da RNP e faz uso do fone@RNP. Naturalmente, cresceram também os pedidos para inclusão de criptografia para as conversações e para a sinalização no fone@RNP.

Sobre o fone@RNP

O fone@RNP é um serviço colaborativo que visa conseguir economia para instituições, tratando questões do serviço telefônico. Ele atua basicamente em duas frentes: transportando ligações a distância por meio da rede Ipê, o *backbone* da RNP, e oferecendo alternativa econômica aos fabricantes tradicionais de PABX, ao prover uma solução de PABX IP em conjunto com proxies SIP (SRLs).

O resumo da arquitetura do serviço pode ser encontrado no capítulo 4 do livro do fone@RNP v2012. O livro também traz introdução à Telefonia e Voz sobre IP, bem como roteiros de instalação e configuração dos módulos que compõem o serviço.



A parte inicial da videoaula sobre o Gateway Transparente (GWT), um módulo do serviço, também faz uma introdução sobre sua arquitetura.

Apresentações

As apresentações serão realizadas nas reuniões do Grupo de Interesse Especial (SIG, em inglês) de Comunicação e Colaboração, parte do novo Sistema de Capacitação e Integração da RNP (SCI). O encontro será realizado remotamente, pelo serviço de Conferência Web, em 27 de setembro de 2017. Estão previstas quatro apresentações de 30 minutos, mais 20 minutos para discussão. Entretanto, esse número pode mudar conforme a oferta de artigos.

Propostas

O modelo para submissão das propostas encontra-se no link http://url.rnp.br?modelo-artigo. Fiquem à vontade para utilizar seus *layouts* de apresentação.

Os interessados podem enviar dúvidas e suas propostas de artigo (com o máximo de seis páginas) até o dia 30 de agosto para sd@rnp.br, com o assunto "SIG de Comunicação e Colaboração - Sigilo no fone@RNP". Não é preciso enviar as apresentações.

Datas importantes:
30/8 - Prazo final para recebimento propostas
13/9 - Divulgação dos trabalhos aceitos
27/9 - Realização do SIG