Relatoria LACIGF 12

Título da sessão: Sessão 8 – Proteção da criptografia e as implicações às comunicações seguras na Internet

Resumo da sessão:

A sessão 8 foi sobre uso da criptografia, começando com uma introdução técnica e depois com a discussão de questões como a regulamentação do seu uso e inclusão de gênero na criptografia.

A primeira palestrante, **Nathalia Sautchuk (Internet Society Brasil, Brasil)**, introduziu a criptografia em termos técnicos. Como motivações para o seu uso, ela apresentação os cenários de aplicações de mensagens instantâneas, *e-commerce* e *internet banking;* prosseguiu-se com a definição de criptografia, baseada nos conceitos de texto claro, texto cifrado, chave e algoritmo. Nathalia também disse que não existe um algoritmo de criptografia 100% seguro, mas é possível alcançar uma possibilidade que seja computacionalmente segura, com base em medições de tempo e de custo necessários para quebrar o sistema criptográfico. Depois de dizer que a segurança por obscuridade não é recomendada, porque é impossível auditar o algoritmo, a palestrante descreveu os algoritmos de criptografia com base no número de chaves (chave pública ou simétrica); no tipo de operação (substituição ou transposição); modo de processamento (bloco ou fluxo). Por fim, Nathalia citou três pontos que devem ser considerados para a avaliação de segurança de um aplicativo: se seu código é aberto; se a criptografia é de ponta-a-ponta; e se há uso de *forward secrecy*, em que uma chave é criada a cada nova sessão.

A moderadora, **Adela Goberna (ALAI, Argentina)**, agradeceu à Nathalia pela sua fala e propôs as perguntas: "Quais são os princípios do uso técnico da criptografia?" e "Qual é o seu custo-benefício?".

Dadas as três propriedades de segurança fornecidas pela criptografia (ou seja, confidencialidade, integridade e autenticidade), a segunda participante do painel, **Veridiana Alimonti (Electronic Frontier Foundation, Brasil)** afirmou que a criptografia também pode ser usada para garantir outros direitos, como a liberdade de expressão. No entanto, ela questionou qual deveria ser a regulamentação da criptografia, argumentando que uma regulamentação incorreta poderia levar a violações de direitos.

Daniela Macías (Direção Nacional de Registro de Dados Públicos, Equador) afirmou que a comunicação é um elemento essencial da tecnologia e, portanto, é muito importante garantir que esse elemento seja seguro. Isso pode ser feito, por exemplo, usando criptografia. Ela também enfatizou a importância e as tentativas de se criar regras para o uso da criptografia, acrescentando que as regras devem ser amplas para não limitar direitos; acrescentou que a criptografia é essencial para garantir a proteção dos dados pessoais, mas esclarecendo que outras medidas devem ser usadas em conjunto com ela, sendo a criptografia apenas uma pequena parte dessa proteção.

María Cristina Capelo (Facebook, México) começou dizendo que a criptografia de ponta-a-ponta é importante para a privacidade e a segurança, mas enfatizando que não é uma tecnologia perfeita, devendo por isso possuir um equilíbrio social. Maria disse que o WhatsApp, um dos produtos que ela representa, usa criptografia de ponta-a-ponta por padrão; e o Messenger, outro produto, permite que esse tipo de criptografia seja habilitado. Maria também afirmou que o usuário deve ter o poder de escolher a plataforma que utilizará. Isso ocorre porque qualquer invasor explorará qualquer vulnerabilidade e o uso de algumas funcionalidades podem gerar essa vulnerabilidade (por exemplo, fazer um backup na nuvem pode comprometer a criptografia).

Angélica Contreras (FemHackPartyLAC e Women SIG, México), em sua fala, foi mais focada em questões de inclusão de gênero no uso da criptografia, afirmando que muitas mulheres são vítimas de violência e vigilância no ambiente digital e que, devido às propriedades de segurança da criptografia, essa ferramenta pode auxiliar em tais casos. Contudo, a palestrante mencionou problemas de alfabetização digital e inclusão linguística, uma vez que muitos documentos de tecnologia criptográficas não estão escritos em diversos idiomas dos povos latino-americanos. Essa falta de diversidade linguística não promove a inclusão digital.

Outputs e outros links relevantes:

- Sessão completa em: https://youtu.be/8TJIzVp_yjE
- Apresentação de Nathalia Sautchuk em: https://www.slideshare.net/nathaliapatricio/conceptos-fundamentales-sobre-el-funcionamiento-y-la-utilidad-del-cifrado

Por: Gabriel Arquelau Pimenta Rodrigues (Universidade de Brasília, Brasil), Flavio Andre Garces Heredia (Colombia)

Traduzido por: Laura Gabrieli Pereira da Silva (UNESP, Brasil)

Revisado por: Pablo Jordan (Internet Society Bolivia, Bolivia)

Coordenação e edição: Nathalia Sautchuk Patrício (NIC.br, Brasil) e Guilherme Alves (Youth Observatory, Brasil)