Artigo final de segurança da informação - Análise da Criptografia Ponta-a-Ponta: Um Estudo sobre o Protocolo Signal e suas implementações

Luiz Antônio Lima de Freitas Leite[1], **Max José Lobato Pantoja Junior**[1], **Wesley Pontes Barbosa**[1]

[1]Instituto de Ciências Exatas e Naturais (ICEN) – Universidade Federal Pará
Belém, PA – Brasil

{luiz.freitas.leite,max.junior,wesley.pontes.barbosa}@icen.ufpa.br

Abstract. *This paper presents an analysis of End-to-End Encryption (E2EE), focusing on the Signal Protocol. It explores its history, cryptographic foundationssuch as the Double Ratchet algorithmand its implementations in global applications. A comparative study is conducted between the original Signal implementation and its integration into WhatsApp, highlighting differences in metadata collection and privacy policies based on official documentation.*

Resumo. *Este trabalho apresenta uma análise da Criptografia Ponta-a-Ponta (E2EE), com foco no Protocolo Signal. Explora-se sua história, fundamentos criptográficos como o algoritmo Double Ratchet e suas implementações em aplicações globais. Realiza-se um estudo comparativo entre a implementação original do Signal e sua integração no WhatsApp, destacando diferenças na coleta de metadados e políticas de privacidade com base em documentações oficiais.*

1. Introdução

A segurança da informação em ambientes de mensageria instantânea evoluiu drasticamente na última década. O Protocolo Signal, desenvolvido pela Signal Messenger LLC, tornou-se a base para a comunicação segura moderna. Este artigo analisa como o protocolo funciona e como grandes empresas, como a Meta, o adaptaram para o WhatsApp, sacrificando parte da privacidade em favor da coleta de metadados.

2. O Protocolo Signal: Origem e Evolução

O Protocolo Signal não nasceu com esse nome. Ele é a evolução do protocolo TextSecure, criado pela Whisper Systems, empresa fundada pelo pesquisador de segurança Moxie Marlinspike. Após a aquisição pelo Twitter e posterior retorno ao modelo open-source, o protocolo foi refinado para o que conhecemos hoje.

Atualmente, o código-fonte está disponível publicamente no GitHub [**?**] e sua documentação técnica descreve um sistema robusto de criptografia ponta-a-ponta (E2EE) que garante que apenas os interlocutores tenham acesso ao conteúdo das mensagens.

3. Arquitetura Criptográfica

O núcleo do Signal baseia-se em três mecanismos principais:

- **X3DH (Extended Triple Diffie-Hellman):** Estabelece uma chave compartilhada entre duas partes que não se conhecem previamente.
- **Double Ratchet Algorithm:** O "coração"do protocolo. Ele renova as chaves de criptografia a cada mensagem enviada, garantindo a *Forward Secrecy* (se uma chave for roubada, mensagens futuras não são comprometidas) e a *Post-Quantum Resistance* parcial.
- **Sesame Algorithm:** Gerencia o estado da sessão em dispositivos múltiplos.

4. Implementações: Signal vs. WhatsApp

Embora o WhatsApp utilize o Protocolo Signal desde 2016 por meio de um acordo com a Open Whisper Systems, as implementações divergem em termos de privacidade de dados periféricos.

4.1. A Questão dos Metadados no WhatsApp

Diferente do aplicativo Signal, que minimiza a coleta de dados ao extremo (armazenando apenas a data de criação da conta e o último acesso), o WhatsApp coleta uma vasta gama de metadados. De acordo com os Termos de Serviço da Meta [**?**], os dados coletados incluem:

- Frequência e duração das interações;
- Identificadores de dispositivo (IP, modelo, sistema operacional);
- Localização aproximada;
- Listas de contatos e logs de transações comerciais.

4.2. Opacidade vs. Transparência

Enquanto o Signal é totalmente *open-source*, o WhatsApp utiliza uma implementação proprietária (fechada) do protocolo. Isso significa que, embora o conteúdo da mensagem seja cifrado pelo Signal, o "envelope"que a carrega (os metadados) é processado pela infraestrutura da Meta para fins de análise e publicidade direcionada.

5. Conclusão

O Protocolo Signal revolucionou a segurança digital. Contudo, sua implementação no WhatsApp demonstra que a criptografia de conteúdo é apenas uma camada da privacidade. A soberania dos dados do usuário depende não apenas do algoritmo, mas da política de metadados da plataforma.

Referências