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 the Signal Protocol, currently considered the gold standard in end-to-end encryption (E2EE) for instant messaging. We discuss its history, evolution from TextSecure and RedPhone, and its technical characteristics, such as the Double Ratchet algorithm and X3DH key agreement. Furthermore, we analyze its most famous implementation: WhatsApp. We examine the partnership between WhatsApp and Open Whisper Systems and highlight the critical privacy differences between the two platforms, focusing specifically on the aggressive metadata collection practiced by WhatsApp compared to the data minimization approach of the original Signal application.*

Resumo. *Este artigo apresenta uma análise do Protocolo Signal, atualmente considerado o padrão-ouro em criptografia ponta-a-ponta (E2EE) para mensagens instantâneas. Discutimos sua história, evolução a partir do TextSecure e RedPhone, e suas características técnicas, como o algoritmo Double Ratchet e o acordo de chaves X3DH. Além disso, analisamos sua implementação mais famosa: o WhatsApp. Examinamos a parceria entre o WhatsApp e a Open Whisper Systems e destacamos as diferenças críticas de privacidade entre as duas plataformas, focando especificamente na coleta agressiva de metadados praticada pelo WhatsApp em comparação com a abordagem de minimização de dados do aplicativo Signal original.*

1. Introdução

A comunicação digital segura tornou-se um requisito fundamental na sociedade moderna. Com o aumento da vigilância em massa e violações de dados, a Criptografia Ponta-a-Ponta (E2EE - *End-to-End Encryption*) surgiu como a principal defesa para garantir a confidencialidade das comunicações. Nesse cenário, o Protocolo Signal destaca-se como a tecnologia mais robusta e amplamente auditada para mensagens assíncronas.

O objetivo deste trabalho é desmistificar o funcionamento do Protocolo Signal, explorando suas raízes históricas e seus mecanismos criptográficos avançados, como o *Perfect Forward Secrecy* (Sigilo Perfeito Encaminhado). Além disso, o trabalho analisa criticamente a dicotomia entre a segurança do conteúdo da mensagem e a privacidade do usuário, utilizando o WhatsApp como estudo de caso para demonstrar como uma implementação segura do protocolo pode coexistir com a coleta extensiva de metadados.

2. História e Evolução do Protocolo

O Protocolo Signal não surgiu como um produto único, mas como a evolução de ferramentas de segurança anteriores. Sua história está intrinsecamente ligada ao criptógrafo Moxie Marlinspike e ao pesquisador Trevor Perrin.

2.1. Origens: TextSecure e RedPhone

Originalmente, a tecnologia foi desenvolvida pela empresa *Whisper Systems*, co-fundada por Marlinspike em 2010. A empresa lançou dois aplicativos para Android: o **TextSecure**, focado em mensagens de texto criptografadas, e o **RedPhone**, focado em chamadas de voz criptografadas.

Em 2011, a *Whisper Systems* foi adquirida pelo Twitter. No entanto, o projeto foi relançado como um projeto de código aberto sob a organização **Open Whisper Systems** (agora sob a égide da *Signal Technology Foundation*). Em 2014, as funcionalidades do TextSecure e do RedPhone foram unificadas, dando origem ao aplicativo Signal como o conhecemos hoje.

3. O Protocolo Signal: Aspectos Técnicos

O Protocolo Signal é um protocolo criptográfico não federado projetado para fornecer confidencialidade de ponta a ponta e integridade de mensagens. O código-fonte do protocolo é aberto e auditável, estando disponível nos repositórios oficiais da organização no GitHub[1].

A robustez do protocolo baseia-se na combinação de diversas primitivas criptográficas modernas, detalhadas na documentação técnica oficial [**?**]:

3.1. O Algoritmo Double Ratchet

O núcleo do protocolo é o algoritmo *Double Ratchet* (Catraca Dupla). Este mecanismo permite que as chaves de criptografia sejam atualizadas constantemente a cada mensagem trocada. Ele combina duas "catracas":

- **Diffie-Hellman Ratchet:** Atualiza as chaves baseada na troca de novas chaves públicas Diffie-Hellman junto com as mensagens.
- **Hash Ratchet:** Deriva novas chaves a partir das anteriores usando uma função de hash (KDF), garantindo que, mesmo se uma chave for comprometida, as mensagens futuras (*Post-Compromise Security*) e passadas (*Forward Secrecy*) permaneçam seguras [**?**].

3.2. Acordo de Chaves X3DH

Para iniciar uma conversa de forma assíncrona (quando um usuário está offline), o protocolo utiliza o *Extended Triple Diffie-Hellman* (X3DH). Isso permite que dois usuários estabeleçam uma chave secreta compartilhada mutuamente autenticada, baseada em chaves pré-publicadas (PreKeys) no servidor, sem que o servidor tenha acesso ao conteúdo da chave final.

[1] `https://github.com/signalapp`

4. Implementações e o Caso WhatsApp

Devido à sua robustez e licença GPLv3, o Protocolo Signal tornou-se o padrão da indústria, sendo adotado não apenas pelo aplicativo Signal, mas também pelo Google (em seu modo RCS), Facebook Messenger (em conversas secretas) e, mais notavelmente, pelo WhatsApp.

4.1. Adoção pelo WhatsApp

Em 2014, logo após ser adquirido pelo Facebook (atual Meta), o WhatsApp firmou uma parceria com a Open Whisper Systems para integrar o protocolo em sua plataforma. O processo foi concluído em abril de 2016, ativando a criptografia ponta-a-ponta por padrão para mais de um bilhão de usuários na época [**?**].

Tecnicamente, o WhatsApp utiliza a mesma base criptográfica do aplicativo Signal. Isso significa que o conteúdo das mensagens (texto, áudio, vídeo) é matematicamente inacessível para a Meta ou terceiros. No entanto, a segurança do conteúdo não implica na privacidade total do usuário.

4.2. Diferenças Críticas: A Questão dos Metadados

Embora o WhatsApp utilize o Protocolo Signal para cifrar o "payload"(conteúdo), o modelo de negócios da Meta baseia-se na coleta de dados. A principal diferença entre o aplicativo Signal original e o WhatsApp reside nos **metadados** os dados sobre os dados.

Enquanto o Signal armazena apenas o dia da criação da conta e a data do último login, o WhatsApp coleta e associa ao usuário uma vasta gama de metadados não criptografados. Conforme descrito em sua Política de Privacidade [**?**], o WhatsApp coleta:

- **Identificadores:** Números de telefone do usuário e de todos os seus contatos (o grafo social).
- **Dados de Uso:** Tempo, frequência e duração das interações.
- **Informações do Dispositivo:** Modelo de hardware, sistema operacional, nível de bateria, força do sinal e identificadores únicos de dispositivo.
- **Endereço IP e Localização:** Dados de localização aproximada baseados na conexão.
- **Dados de Transação:** Se o usuário utiliza serviços de pagamento no app.
- **Informações de Grupo:** Nomes de grupos e fotos de perfil (que não são criptografados ponta-a-ponta da mesma forma que as mensagens).

Essa coleta permite que a Meta construa perfis comportamentais detalhados, sabendo "quem fala com quem, quando e de onde", mesmo sem ler o conteúdo das mensagens. No aplicativo Signal, a arquitetura é desenhada para "Sealed Sender"(Remetente Selado), ocultando até mesmo quem está enviando a mensagem dos servidores de roteamento sempre que possível.

5. Conclusão

O Protocolo Signal representa o estado da arte na segurança de comunicações móveis. Sua adoção pelo WhatsApp foi um marco histórico que democratizou a criptografia forte para bilhões de pessoas. Contudo, este estudo evidencia que a criptografia ponta-a-ponta,

embora vital para a confidencialidade do conteúdo, não protege os metadados. A comparação entre as implementações do Signal e do WhatsApp demonstra que a privacidade real depende tanto da robustez dos algoritmos quanto das políticas de coleta de dados da organização que detém a infraestrutura.

Referências