Projeto de Formatura – Turmas 2018

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema:

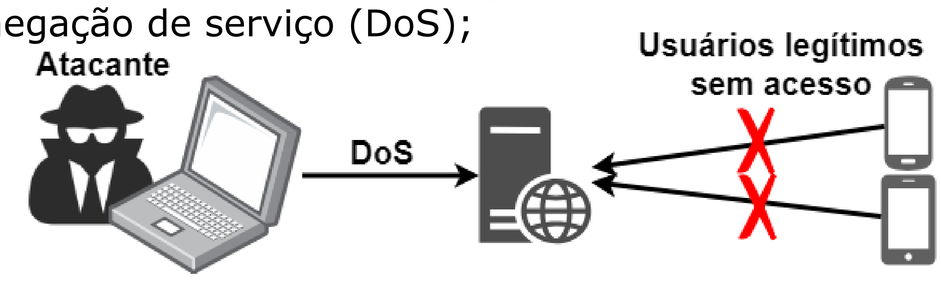
***Eri-chain* : aplicativo de troca de mensagens instantâneas factível de auditorias e distribuído**

MOTIVAÇÃO E OBJETIVO

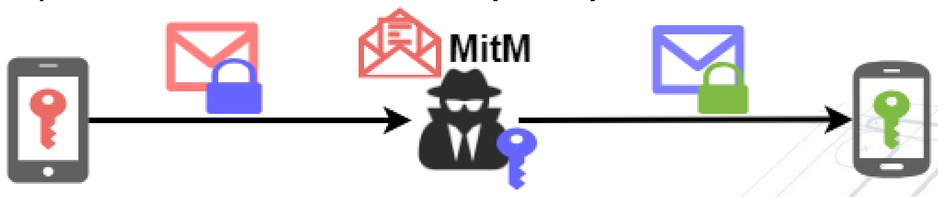
Aplicativos de troca de mensagem instantâneas estão sendo utilizados para comunicação profissional, por isso é necessário ter registros confiáveis das conversa.

Maioria dos aplicativos são centralizados e apresentam vulnerabilidades:

- pontos únicos de falha lógica, alvos de ataques de negação de serviço (DoS);



- gerenciamento de chaves públicas por parte da entidade central pode permitir que esta realize ataque de homem-no-meio (MitM).



- Falta de mecanismos integridade das conversas em relação ao conteúdo e a sequência das mensagens.

Conversa original	Conversa modificada (Ordem das mensagens alterada)
A: Você frequenta academia? B: 3 vezes por semana. A: Você fuma? B: Não	A: Você frequenta academia? B: Não. A: Você fuma? B: 3 vezes por semana.

Visando mitigar as vulnerabilidades, propõe-se neste trabalho uma arquitetura P2P com segurança fim-a-fim, de forma a tornar a aplicação mais independente e garantir a integridade e autenticidade das conversas realizadas via aplicativos celular.

TRABALHOS RELACIONADOS

Telegram

- Preocupou-se em colocar suporte à criptografia fim-a-fim desde a criação, mas não é habilitada por padrão;
- Algoritmo de segurança de autoria própria;
- Código parcialmente fechado;
- Arquitetura centralizada.

WhatsApp

- Incorporou criptografia fim-a-fim em 2016;
- Código fechado;
- Servidor gerencia as chaves públicas;
- Testes mostraram que o protocolo de segurança não foi devidamente implementado no app [1];
- Arquitetura centralizada.

Signal

- Código aberto;
- Arquitetura centralizada.

***Briar* [2]**

- Código aberto;
- Arquitetura distribuída;
- Privacidade;
- Esquema anti-censura.

Integrante:

Andrea Erina Komo

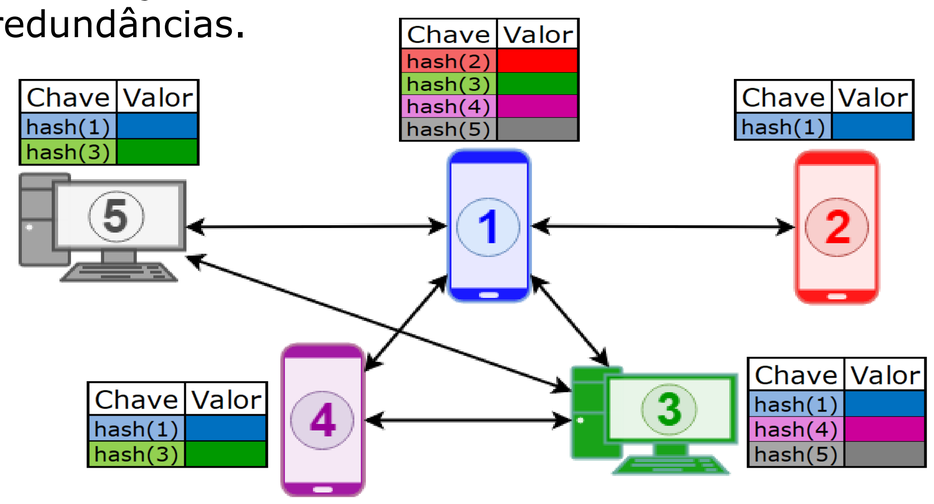
Professor Orientador:

Prof. Dr. Marcos Antonio Simplicio Junior

ARQUITETURA PROPOSTA

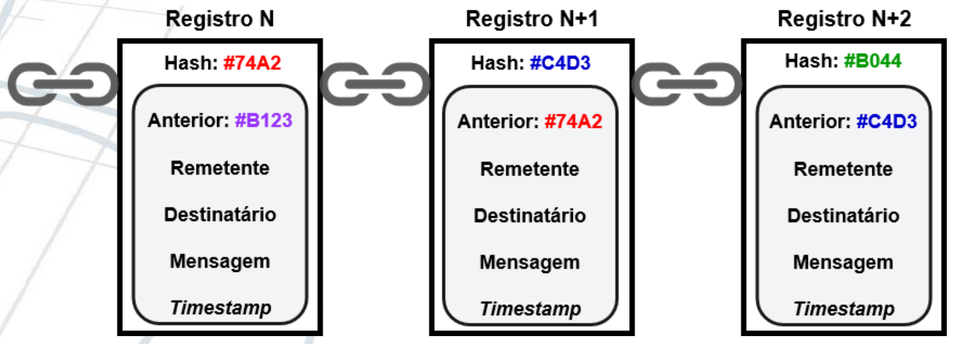
Rede de conexão: DHT (*Distributed Hash Table*)[3]

- Armazena informações de conexão dos usuários (IP e porta, chave pública PGP e o certificado digital) em pares (`chave`, `valor`).
- Informações distribuídas entre os nós da rede com redundâncias.



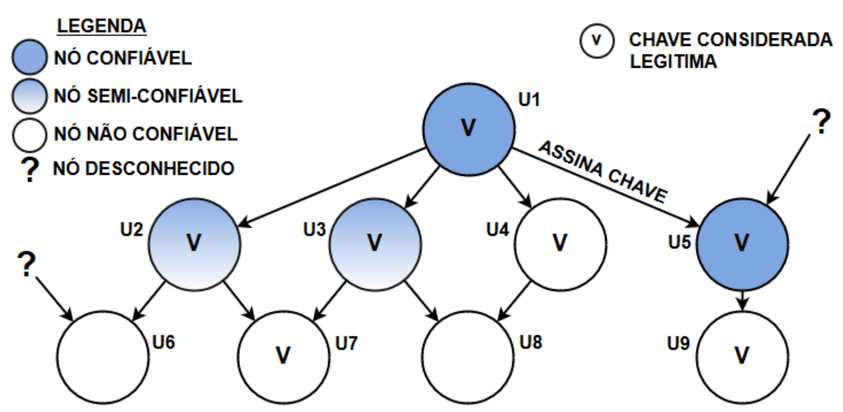
Estrutura de segurança: *hash chain* [4]

- Registros íntegros, ordenados e confiáveis.



Estrutura de segurança: PGP [5]

- RFC 4880: OpenPGP [6]
- Rede de confiança



CONCLUSÃO

Rede de conexão é independente e resistente à censura.

Usuários podem atribuir graus de confiança diferentes para as chaves públicas.

Estabelecimento de conexões móveis seguras.

Sistema garante integridade e autenticidade das mensagens e da conversa.

Protótipo desenvolvido:

- Sistema Android v6.0 ou superior
- Código disponibilizado em repositório no GitHub: https://github.com/Erina-chan/eri-chain

REFERÊNCIAS

[1] Boelter, T. (2016). *WhatsApp Retransmission Vulnerability*. Disponível em: https://tobi.rocks/2016/04/whats-app-retransmission-vulnerability/.

[2] Rogers, M. et al. Briar. 2018. Disponível em: https://briarproject.org/.

[3] Zhang, H.,Wen, Y., Xie, H., and Yu, N. (2013). *A Survey on Distributed Hash Table (DHT): Theory, Platforms, and Applications*.

[4] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

[5] Zimmermann, P. (1995). *Building in Big Brother. chapter Pretty Good Privacy: Public Key Encryption for the Masses*, pages 93–107. Springer.

[6] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. (2007). *RFC 4880: OpenPGP Message Format*. https://tools.ietf.org/html/rfc4880.