Um sistema de criptografia de broadcast para navegadores de internet

Motivação

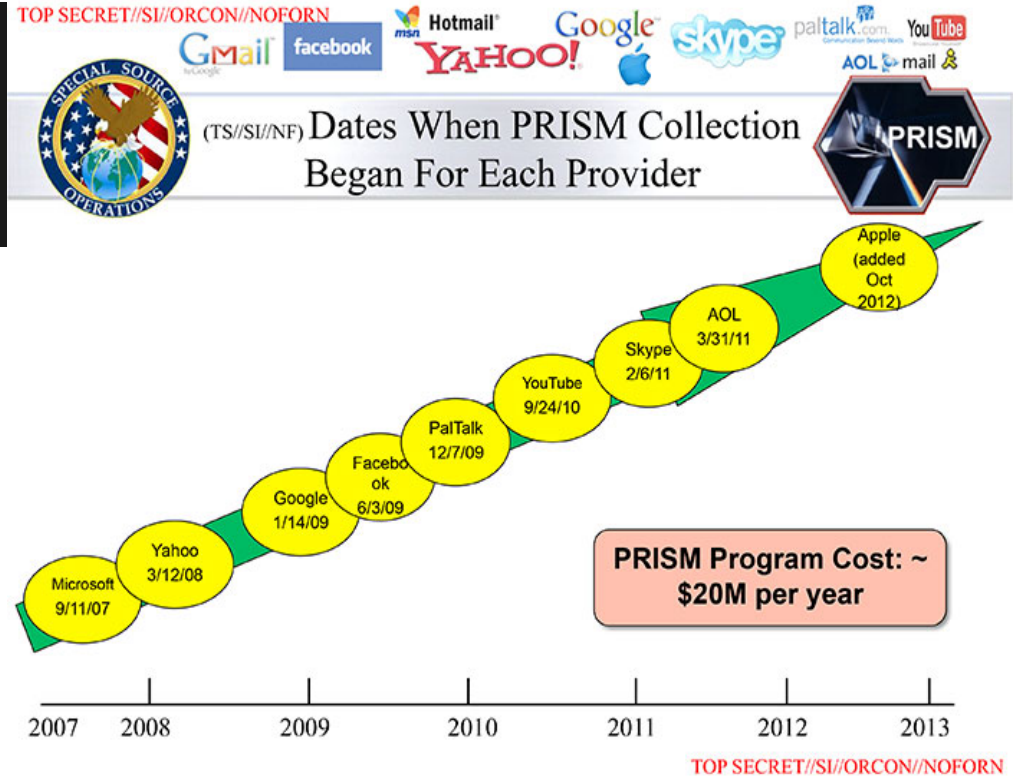
- HTTPS

Motivação

- HTTPS
- Dados no servidor

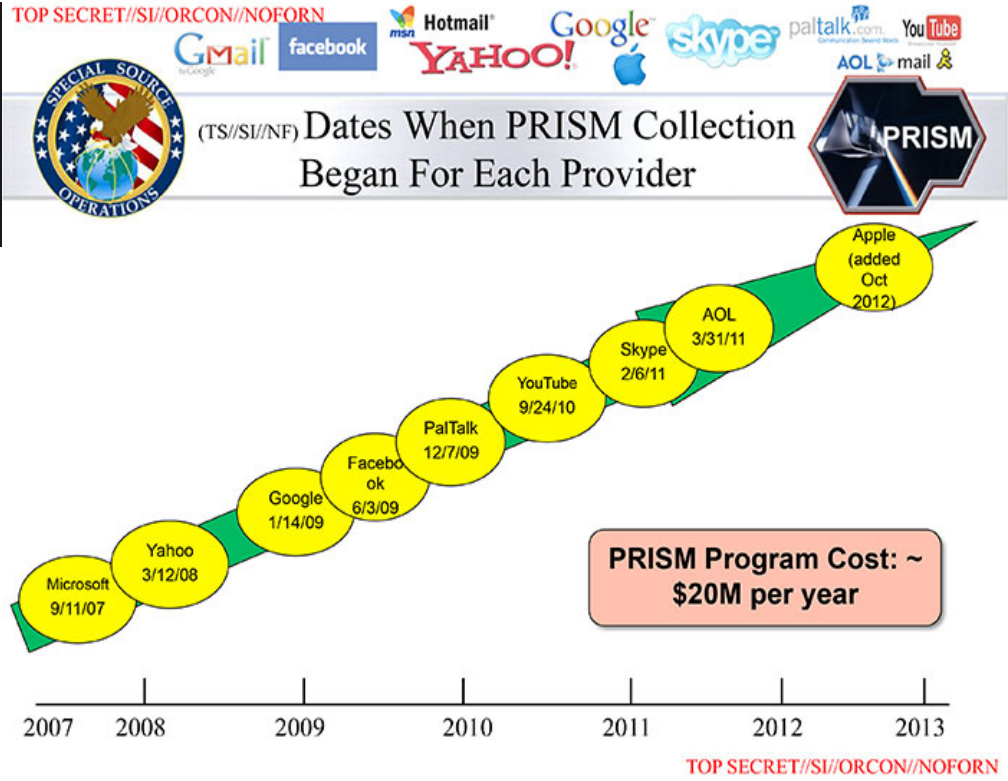
Motivação

- HTTPS
- Dados no servidor
- PRISM



Motivação

- HTTPS
- Dados no servidor
- PRISM **BREAK**



Motivação

Um sistema para e-mail

Motivação

Um sistema para e-mail

Um sistema para chat

Motivação

Um sistema para e-mail

Um sistema para chat

Um sistema para conferência

Motivação

Um sistema para e-mail

Um sistema para chat

Próprio usuário tem que gerenciar as chaves

Um sistema para conferência

Motivação

Um sistema para e-mail

Exige conhecimento técnico "não trivial"

Um sistema para chat

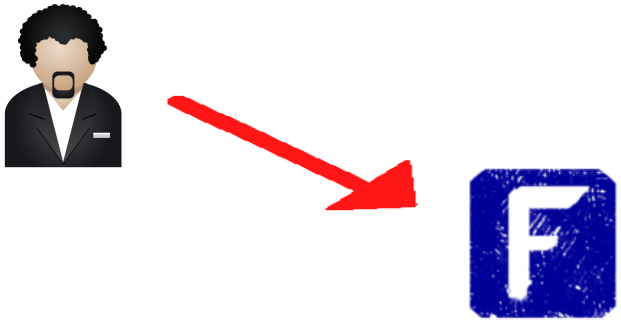
Próprio usuário tem que gerenciar as chaves

Um sistema para conferência

Proposta

- Sistema geral
- Poucos pré-requisitos
- Não interfira na experiência
- Proteja os dados também dos servidores

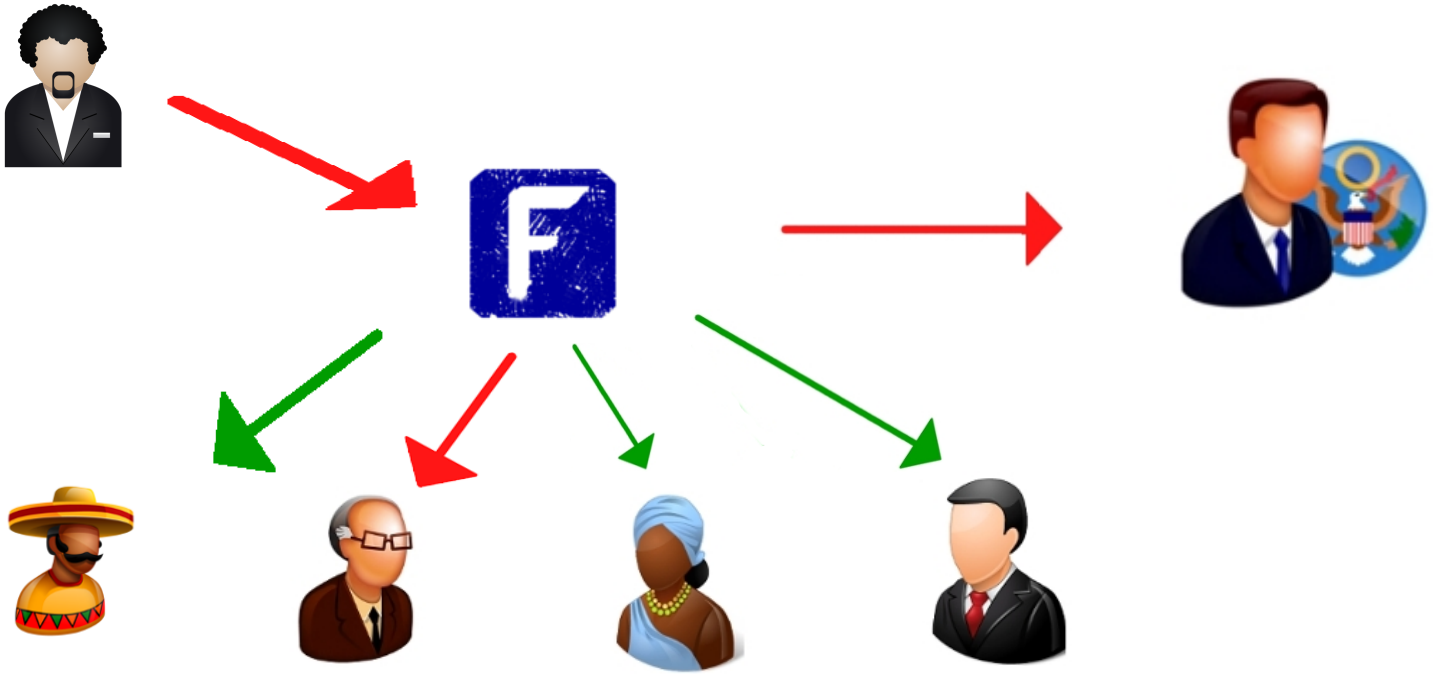
Funcionamento



Funcionamento

Funcionamento

Funcionamento



Funcionamento

N_1  (A_1, X_1)

N_2  (A_2, X_2)

N_3  (A_3, X_3)

Funcionamento

Chave de sessão : S

N_1  (A_1, X_1)

N_2  (A_2, X_2)

N_3  (A_3, X_3)

Funcionamento

Chave de sessão : S

Criptografa S com as chaves públicas dos contatos :
R_k = Elgamal (A_k,S)

N_1

(A_1, X_1)

N_2

(A_2, X_2)

N_3

(A_3, X_3)

Funcionamento

Resolve o sistema de equações modulares:

$$X = R_k \pmod{N_k} \quad (k=1,2,3)$$

(Teorema Chinês do Resto)

N_1  (A_1, X_1)

N_2  (A_2, X_2)

N_3  (A_3, X_3)

Funcionamento

Para enviar uma mensagem M :

C = AES (M, S)

e envia : (X, C)

N_1  **(A_1, X_1)**

N_2  **(A_2, X_2)**

N_3  **(A_3, X_3)**

Funcionamento

Para descriptografar uma mensagem (X, C) :

$$R_k = X \pmod{N_k}$$

$$S = ElGamal\ (X_k,\ R_k)$$

$$M = AES\ (S, C)$$

N_1  (A_1, X_1)

N_2  (A_2, X_2)

N_3  (A_3, X_3)

Funcionamento

Remover/Adcionar contato :

Basta recalcular os R_k e resolver um novo sistema de esquações modulares

$$X = R_1 \pmod{N_1} \quad e \quad X = R_3 \pmod{N_3}$$

N_1

(A_1, X_1)

(A_2, X_2)

N_3

(A_3, X_3)

Créditos

- Ícones :

  www.icons-land.com e www.aha-soft.com

- Slide do programa PRISM :

  http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Principais referências

- FIPS-197, *Advanced Encryption Standard (AES)*, Novembro de 2001
- Guang-Huei Chiou e Wen-Tsuen Chen, *Secure Broadcasting Using the Secure Lock*, IEEE, Vol. 5, Nº 8.
- Hilder Vitor Lima Pereira, *Algorithmes de cryptographie et le problème du logarithme discret.* Wikimedia Commons, 2012.
- Mozilla Foundation, *Add-on Developer Hub*, https://addons.mozilla.org/en-US/developers/