



# Uma Primeira Análise do Ecossistema HTTPS no Brasil

Thiago Escarrone, Diego Kreutz, Maurício Fiorenza  
4o. Workshop Regional de Segurança da Informação (2019)

# Roteiro

**Motivação**

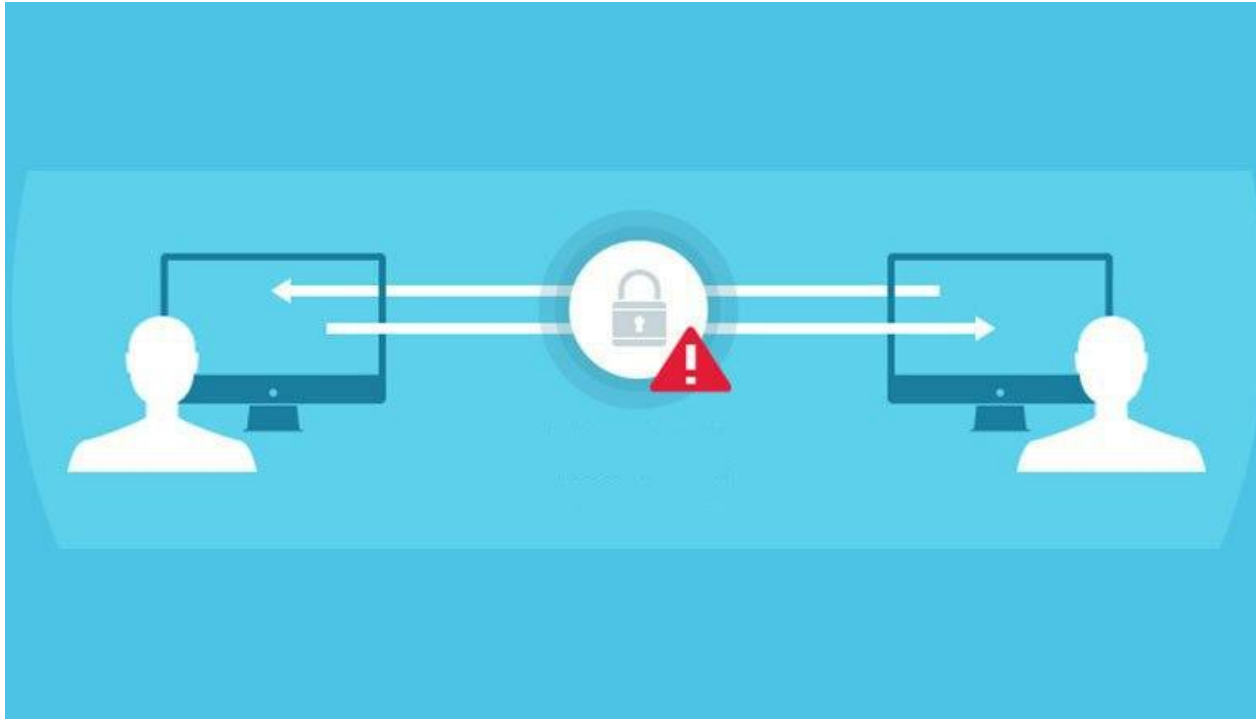
**Navegação segura**

**O Ecossistema HTTPS no Brasil**

**Considerações e Trabalhos Futuros**

# Motivação

- Nós realmente estamos seguros na Internet?



# Motivação

- Será que você está realmente seguro usando HTTPS?



# Roteiro

**Motivação**

**Navegação segura**

**O Ecossistema HTTPS no Brasil**

**Considerações e Trabalhos Futuros**

# HTTP vs HTTPS

## ● HTTP

- Texto puro
- Fácil interceptação e alteração dos dados



## ● HTTPS

- Texto encriptado
- Confidencialidade
- Integridade
- Autenticidade



# HTTPS



**HTTP + SSL = HTTPS**

Hypertext Transfer  
Protocol

Secure Socket  
Layer

Hypertext Transfer  
Protocol Secure

# SSL e TLS

- Fornece confidencialidade e integridade dos dados em uma comunicação





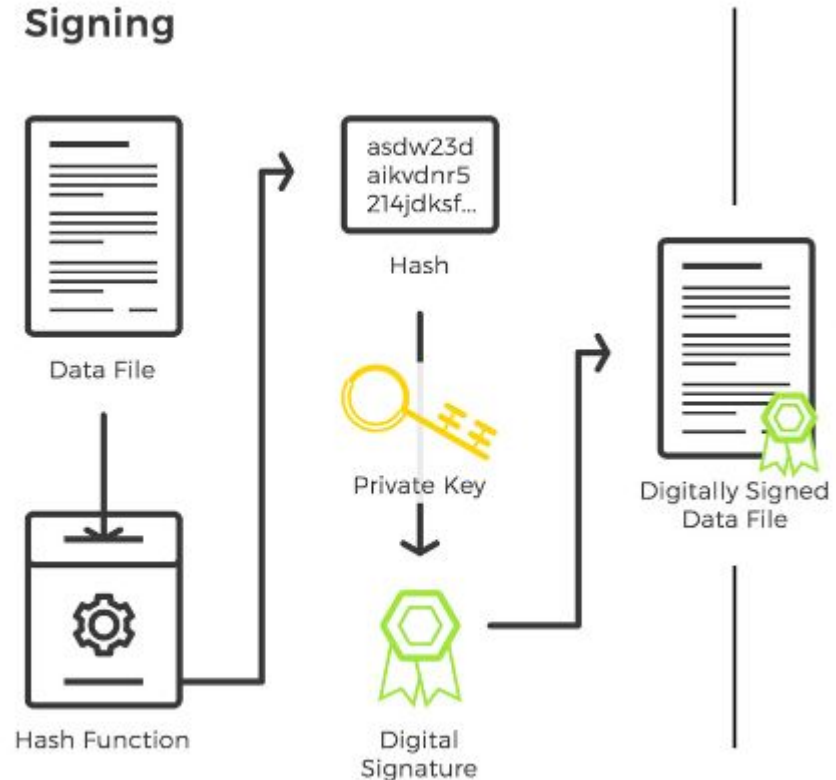
# Autenticidade

- **Certificado Digital**
  - Autoridade Certificadora
  - Nome da empresa
  - Common Name
  - Validade (Not before and Not after)
  - Algoritmo de assinatura



# Algoritmo de Assinatura

- Fornece autenticidade, integridade e não-repúdio



# Roteiro

**Motivação**

**Navegação segura**

**O Ecossistema HTTPS no Brasil**

**Considerações e Trabalhos Futuros**

# Esferas analisadas

- Governo Federal
- Governos Estaduais
- Bancos e fintechs brasileiras

# Não utilizam Certificado Digital

GOOGLE TECH CYBERSECURITY

## Chrome will mark all HTTP sites as 'not secure' starting in July

16

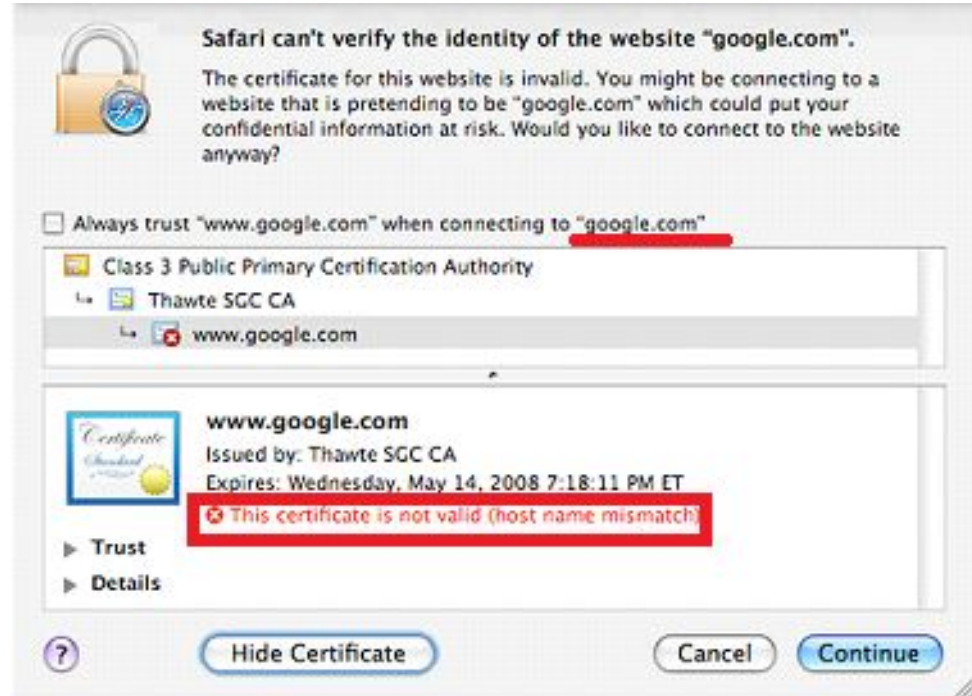
*Google sends a nudge toward the unencrypted web*

By [Russell Brandom](#) | Updated Feb 8, 2018, 1:21pm EST

- 33% dos sites não utilizam HTTPS em suas comunicações

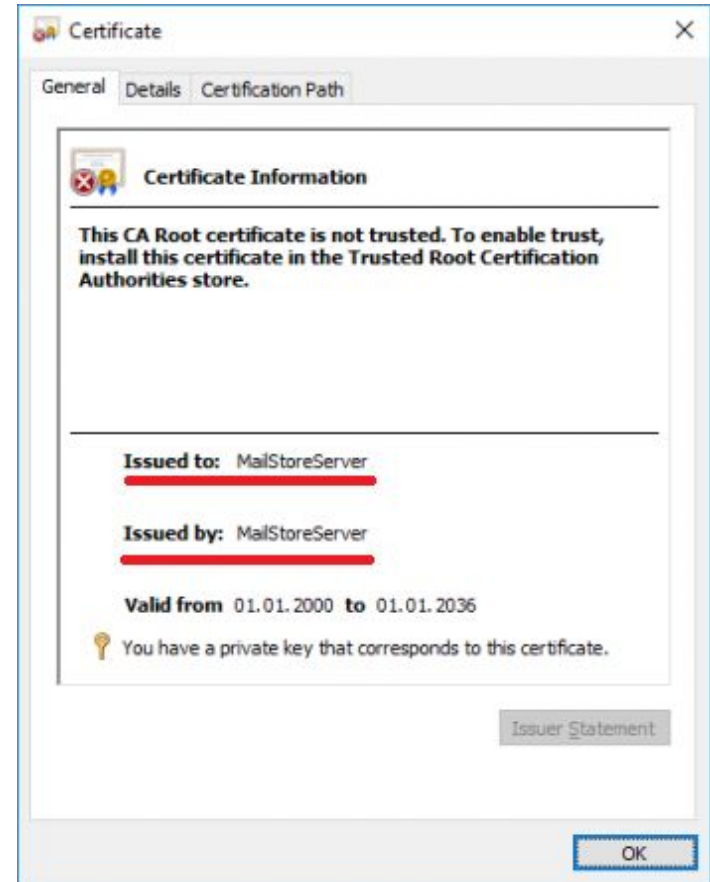
# Domain Name Mismatch

- Endereço acessado != Domínio registrado no certificado
- 20,58% dos sites indicados como não confiáveis



# Certificados Auto-assinados

- Autoridade Certificadora ==  
Nome da empresa
- 14,70% não tem a confiança do navegador



# Certificado fora da data de validade

- Data atual < Not before **AND** Data atual > Not after
- 8,82% dos sites analisados



## O certificado de segurança do site expirou.

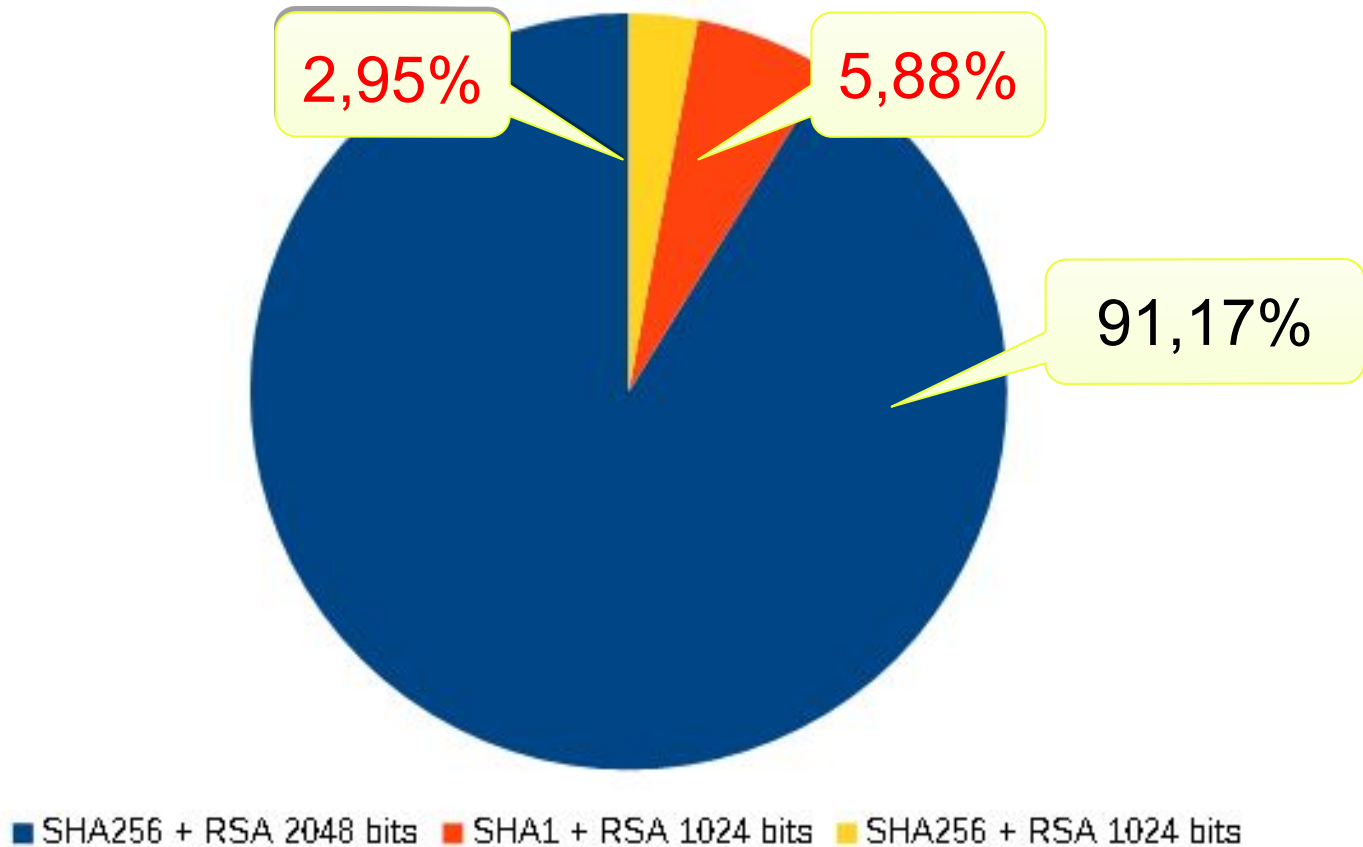
Você tentou acessar **accounts.google.com**, mas o servidor apresentou um certificado expirado. Nenhuma informação está disponível para indicar se o certificado foi comprometido desde a expiração. Isso significa que o Google Chrome não pode garantir que você está se comunicando com **accounts.google.com**, e não com um invasor. O relógio do computador está definido como sexta-feira, 14 de março de 2014 06:11:58. Isso está correto? Caso contrário, você deve corrigir o erro e atualizar esta página.

Você não deve continuar, **principalmente** se nunca tiver visto este aviso antes neste site.

[▶ Mais informações](#)



# Algoritmos de assinatura



# Versão dos protocolos SSL/TLS

Versão	Sites que suportam	Ataques conhecidos
SSLv2	1	DROWN
SSLv1	6	POODLE, BEAST
TLS 1.0	28	BEAST
TLS 1.1	25	POODLE
TLS 1.2	29	Logjam
TLS 1.3	2	-

# Roteiro

**Motivação**

**Navegação segura**

**O Ecossistema HTTPS no Brasil**

**Considerações e Trabalhos Futuros**

# Considerações finais

- Implantações dos certificados digitais precárias(onde tem)
- Versões vulneráveis do SSL/TLS ainda em uso
- Funções Hash antigas ainda em uso

# Trabalhos futuros

- Um número maior de sites (e.g *e-commerce* brasileiro, prefeituras municipais, mais bancos)
- Estudar como os ataques são realizados



# Obrigado!

**Contatos:**

[thiago.escarrone@gmail.com](mailto:thiago.escarrone@gmail.com)

[diego.kreutz@unipampa.edu.br](mailto:diego.kreutz@unipampa.edu.br)

[mauricio.fiorenza@unipampa.edu.br](mailto:mauricio.fiorenza@unipampa.edu.br)