



Uso do HTTPS no Brasil: um estudo abrangente

Thiago Escarone, discente, Universidade Federal do Pampa
Maurício Fiorenza, discente, Universidade Federal do Pampa
Diego Kreutz, docente, Universidade Federal do Pampa
thiagoescarone.aluno@unipampa.edu.br

Em 2019, iniciamos um estudo sobre o ecossistema HTTPS no Brasil. Publicamos um resumo no SIEPE daquele ano, analisando 44 sites. Constatamos que 100% dos sites utilizam uma versão do protocolo TLS vulnerável, ou nem utiliza HTTPS. Dando continuidade à pesquisa, em 2020, aumentamos o escopo das nossas análises para 5806 sites, um salto significativo em termos de representatividade, adicionando instituições financeiras, sites do comércio eletrônico e sites das três esferas governamentais (municipal, estadual e federal). A simples utilização do HTTPS não é sinônimo de segurança. Um site pode utilizar HTTPS e continuar absolutamente inseguro no contexto de segurança cibernética dos dias atuais. A segurança do HTTPS é mantida pelo TLS, que oferece segurança em camada de transporte. Entretanto, com exceção da versão mais recente (TLS 1.3), todas as demais versões (e.g., 1.0, 1.1, 1.2), ainda aceitas e suportadas por muitos sites, sofrem de vulnerabilidades que podem comprometer a segurança e privacidade dos dados dos usuários da Internet. Há diferentes ataques conhecidos, como BEAST e POODLE, nas versões inferiores a 1.3 do TLS. O ataque BEAST, por exemplo, possibilita ao atacante acesso a conteúdos sensíveis de um cookie do navegador do usuário, levando, inclusive, ao sequestro da sessão. O que procuramos responder é qual é o estado da saúde do ecossistema HTTPS no Brasil levando em consideração sites de diferentes segmentos, como financeiro, comércio eletrônico e governo? Para a identificação e seleção dos 5806 sites, foram utilizadas as bases de dados e informações da ABCOMM - Associação Brasileira de Comércio Eletrônico (4458 sites), Censys (994 sites), Febraban - Federação Brasileira de Bancos (99 sites) e dados públicos sobre os principais órgãos do governo federal (20 sites), sites de todos os estados da federação (108 sites) e prefeituras municipais (127, selecionadas de maneira pseudo-aleatória). Para a análise dos sites, foi implementado um programa para processar automaticamente os sites utilizando a ferramenta testssl.sh. A partir dos dados coletados, conseguimos identificar que apenas 35% dos sites suportam o TLS 1.3. Entretanto, estes e todos os demais sites ainda suportam versões anteriores do TLS. Isto é um problema de segurança grave, uma vez que 100% dos sites irão, invariavelmente, colocar os usuários em risco devido ao fato de estarem vulneráveis aos ataques conhecidos das versões mais antigas do TLS. Do total, 18% dos sites apresentam também problemas relacionados à implantação do certificado digital, que é algo necessário para estabelecer uma conexão HTTPS confiável. Em resumo, os resultados indicam que há um caminho longo até conseguirmos estabelecer uma cadeia maior de confiança nos sites HTTPS do Brasil. Como trabalho futuro, esperamos analisar dezenas de milhares de sites brasileiros, aumentando a amostragem e precisão das análises.

Agradecimentos: Fomento: UNIPAMPA. Formação e iniciação à pesquisa: projeto de Segurança e Dependabilidade de Sistemas e Dados (SIPPEE 20180316185234).

Palavras-chave: HTTPS, TLS, segurança, Internet, sites